Cyber Security and Android Hacking; An Awareness for Android Users

Syeda Tooba Kazmi*
Department of Computer Science and Software Engineering, Jinnah University for Women, Karachi, Pakistan
*Email: stooba1314@gmail.com

ABSTRACT

In this advanced era of technology, where we have a number of gadgets and applications that on one side provide us comfort and on the other side, a quick access to data, activities and people, we are under a huge compromised zone of privacy and security. Cybercrimes are rising that lead to the exploitation of vulnerabilities of systems being used by the users and hence data is at risk. There is a great number of people that are android users. Hackers therefore try to exploit the vulnerabilities of the android system so as to cover a wide range of devices. This paper focuses on the hacks (using Metasploit framework) that could compromise the security of an android system and shows the results of the attack on the compromised system.

Keywords: Android security, Cybercrimes, Metasploit framework.

INTRODUCTION

The internet and web has become a very important and crucial part of our everyday life with a large number of users all around the world. There are billions of android users, among them are home users and non-home users. Majority of the home users are not aware about the security risks posed to their data, being connected via internet as opposed to the non-home users who are forced by their organizations to make themselves aware of information security and to apply a wide range of information security awareness tools (Kritzinger and Solms). There are various cybercrimes that are committed which can result in compromised security of devices. Since mobiles are easily accessible by majority of the people, therefore, the hackers try to get into the android systems and breach data. Along with bluetooth, WiFi there are various technologies for mobile networks, such as Near Field Communication (NFC) which is a protocol for the communication of devices but it also has potential vulnerabilities (Bermejo, Flores and Hui). A study shows, that users of smartphones can uniquely be identified through the device configurations of their devices. These configuration features are actually collected by the third party app through its official SDK (Kurtz, Gascon and Becker). There are in fact, far going consequences of android hacking. In other words, the attacker can not only access personal information, but it can further breach data and compromise others' confidentiality by accessing social contacts, activities, geo-location, webcam, video streaming and users' communication etc.

OBJECTIVES

The objective of this paper is to put light on the weaknesses and vulnerabilities present in the android system. It warns the users against downloading arbitrary files or opening spam emails, links etc. There is a great threat posed to the web based android users (mobile fingerprinting) as discussed by (Hupperich, Maiorca and Kuhrer). The main objective of this study is to depict the practical approach of compromising the victim's phone and accessing the messages, phone records, phone book and microphone, web cam and photo gallery. This paper depicts a particular type of android hack using the metasploit framework so that the users might get an insight regarding android hacking and also secure themselves against such types of attacks. Although, this attack does not require any third party app to be installed in the victim's phone, but one can carry out attacks on the android systems that use third party applications such as Whatsapp as by injecting a malicious .apk file into the system (Zaabi).

METHODOLOGY

The Metasploit framework, built-in Kali Linux, provides us the environment to hack an android phone. This attack is carried out when it is known that the linux machine (attacker) and the android phone (victim) that is to be hacked, are be on the same network. The network on linux machine should be set to Bridged adapter.

This attack as discussed uses the Metasploit framework built into Kali-Linux to create .apk file that will allow a back door into the user's phone. The script creates the malicious APK file and embeds it into a normal, unsuspicious APK. Once the user, downloads and runs the attached file, i.e. when this .apk file is opened, it will automatically trigger a Perl script to create a persistent backdoor into the victim's phone. At this point, the victim's phone is compromised. To send the infected file to the victim so that it gets downloaded, there are two ways, over the local area network (LAN), or the attacker can open a port for the data to be sent to and listen on the local binding for the data coming in. These options can be specified during the process of the script, creating the APK.

After launching this attack, not only the attacker can easily access the victim's phone but can also carry out various operations on it like capturing screen shot and sending text messages (sms) from it. The Android Meterpreter allows to do tasks like take remote control the file system, listen to phone calls, retrieve or send SMS messages, geo-locate the user, run post-exploitation modules, etc.

RESULTS

After the attack has been launched, the victim's phone is now compromised. The attacker can access the user's data. At this point, using the 'help' command, lists down all the other commands that can be executed by the attacker to compromise the system further. The details of the android system (model, rooted device etc) can be also be found. The attacker can have a list of all the messages on the victim's phone along with the date/ time details (figure 1) using the 'dump_sms' command. The attacker can also send a message to any recipient and it would appear as if it had been sent by the victim. The attacker can gain access to the call logs and phone book as well. This command compromises the victim's privacy as well as that of the other users since the contact details of the latter are also in access of the attacker. The attacker can capture screenshots by using the mobile phone camera (figure 2) and can also start live video streaming. It can also begin live voice recording using the microphone by executing the command 'record_mic' with the victim being least aware of it.

Although, the attack demonstrated above, requires both the attacker and victim to be on the same network, but it can also be launched if they are not on the same network with some additional settings done.

CONCLUSION

The Metasploit framework, built-in Kali Linux, provides us the environment to hack an android phone. In this way, an attacker, can access the data of the mobile phone and also can take control over it. Security risks posed to the android users are not less. The users who have no knowledge of information security must still be very cautious in this regard as a little carelessness might result in compromised privacy. The very basic principle to minimize the risk of an android system being hacked is to avoid downloading anything from untrusted sites or opening links sent by third parties (usually promotional emails). Accessing such vulnerable links/ sites or downloading such apps may attach a virus with them automatically thus compromising the security and privacy of the user.

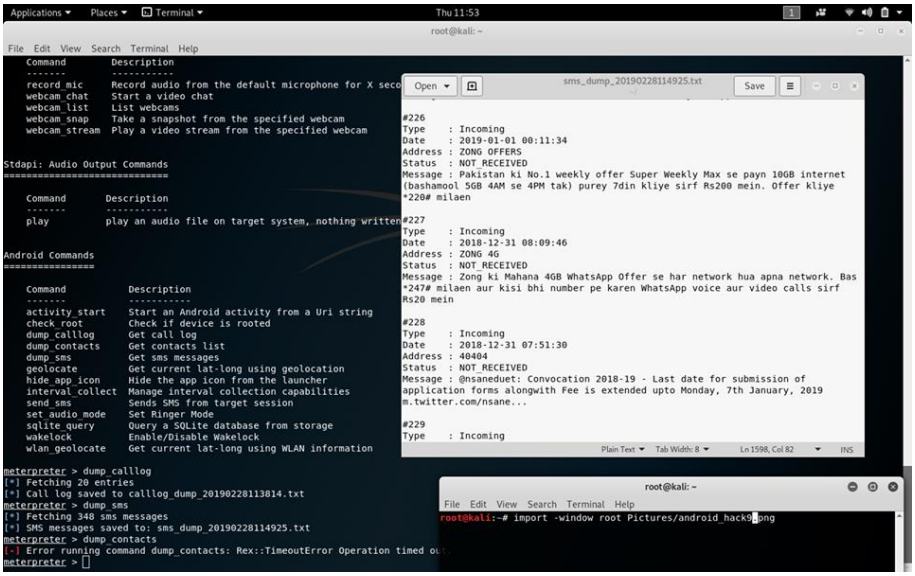

Figure 1. Messages in the victim's phone accessed by the attacker.

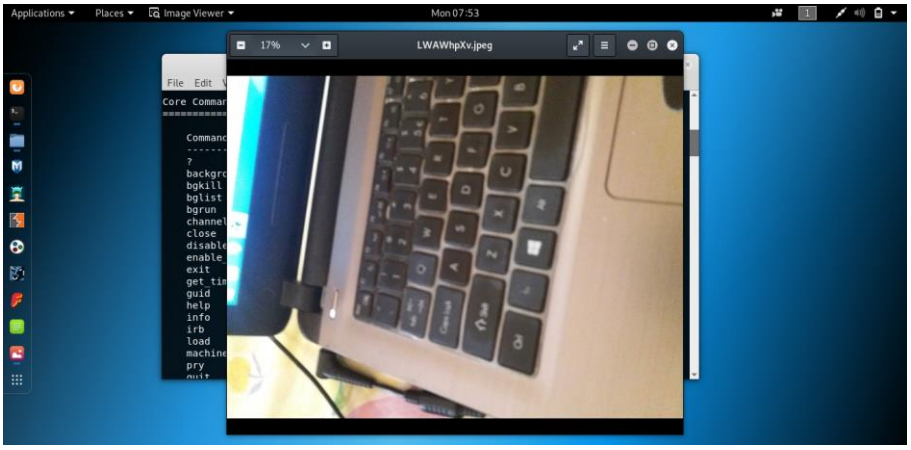

Figure 2. Snapshot captured by the attacker from the victim's webcam.

REFERENCES

1. Bermejo, Carlos, Huber Flores and Pan Hui. "Steal Your Life Using 5 Cents: Hacking Android Smartphones with NFC Tags." International Conference on Pervasive Computing and Communications Workshops. Austin, TX, USA: IEEE, 2020. 1-6.
2. Hupperich, T., *et al.* "On the Robustness of Mobile Device Fingerprinting: Can Mobile Users Escape Modern Web-Tracking Mechanisms?" Proceedings of the 31st Annual Computer Security Applications Conference. Los Angeles, CA, USA: ACM, 2015. 191-200.
3. Kritzinger, Elmarie, and Sebastiaan H. von Solms. "Cyber security for home users: A new way of protection through awareness enforcement." Computers & Security 29.8 (2010): 840-847.
4. Kurtz, Andreas, *et al.* "Fingerprinting mobile devices using personalized configurations." Proceedings on Privacy Enhancing Technologies 2016.1 (2016): 4-19.
5. Al Zaabi, Khulood. "Android device hacking tricks and countermeasures." 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF). IEEE, 2016.