ANDROID MOBILE HACKING USING METASPLOIT

[1] Cherukuri Rahul [2] Vallepu Harsha Vardhan [3] Kittu Praveen Kumar
[4] Dr.V. Shanmukha Rao
[1,2,3] Department of Information Technology, Andhra Loyola Institute of Engineering and Technology.
[4] M. TECH, PHD. Associate Professor Department of Information Technology, Andhra Loyola Institute of Engineering and Technology

1.ABSTRACT

Today, there are more than 6.1 billion smartphone users globally, which equates to approximately a smartphone per user. Out of the 2.6 billion smartphones, almost 4.2 billion of those are Android devices. Android is a mobile operating system built on the Linux kernel. As a result, the smartphone will increasingly be the focus of security measures because it can reveal a great deal of information about the user and serve as a gateway to a company's network. Since Android is the most popular operating system, many mobile apps have malware including spyware, backdoors, trojan horses, etc. We'll create a payload with MSF Venom then save it as an apk file.

2.INTRODUCTION

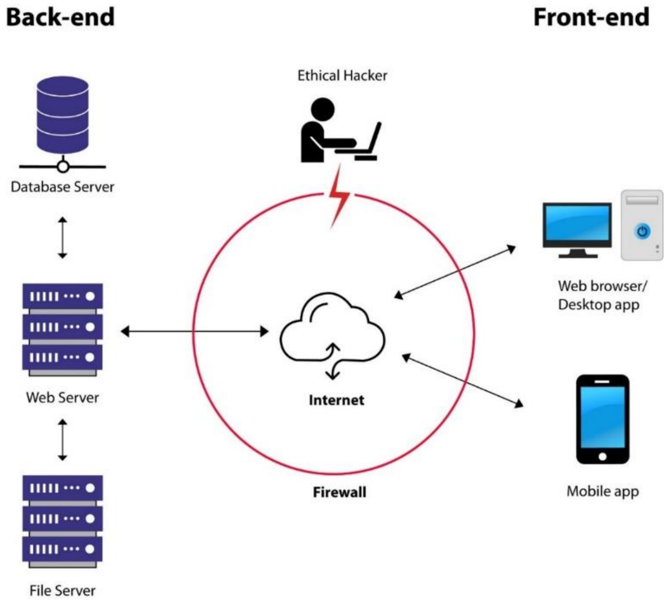
People are becoming more and more reliant on computers, information technology, and security in the modern era. Society and the IT sector are overly concerned about the information on the Internet. One of the main challenges in the IT industry is security infrastructure and software. Even minute details on the Internet are now recorded in the database of computer systems connected to the Internet. Security professionals have created a variety of high-performance security tools to guarantee that the information is safe, secure, and does not have any vulnerabilities, as well as that it conforms with the assigned security requirements. Penetration testing, Assurance or Proof of Correctness, Software Engineering Environment, and Layered Design are some methods. The Entire operational, integrated, and dependable computer base, which consists of software, must be tested using the important technique of penetration testing. More than 1,600 exploits and 495 payloads have been used in penetration testing using open-source frameworks (such Metasploit for exploit creation). By simulating illegal access to the system with the help of a manual process, automated tools, or a mixture of the two approaches. "Mitigating Cyber Security Attacks by Being Conscious of

Vulnerabilities and Bugs" describes how to deal with cyber security attacks by raising knowledge of risks and vulnerabilities. attack methods and vulnerability prevention techniques. The article "Protection against penetration assaults using Metasploit" analyses script-based attacks, employs Metasploit attacks, and conducts an analysis of scripts and payloads in order to create a defense script. The instructions and lists of tools given by Kali Linux 2017.3 are described in "Using Kali Linux Security Tools to Build Laboratory Projects for Cybersecurity Education," which employs preconfigured and preloaded tools for laboratory projects utilizing VMware (virtual machine framework). The purpose of "Offensive Security: Ethical Hacking Methods on the Web" is to plan methodology, generate security assurance policies, and ISO 2007 attacks, risk analysis using MSAT 4.0 tool based on ISO standard. To hack Android phones, tablets, and other devices, we will use Metasploit. You will see that once the Android device has been compromised, we are able to gather the target's text messages, contact list, location, and even activate their webcam!

3. LITERATURE SURVEY

Symantec research states that more than a million cyberattacks take place daily. Both newly developed and existing systems must go through security testing at some point in their lives. There are different approaches available to help testers choose, devise, and implement the best testing processes for diverse circumstances. Each technique typically arises from the unique requirements of a particular type of actors, and as a result, it is slanted towards a particular topic of distinctive interest to them. The most widely used approaches are compared in this article to highlight their advantages. With an emphasis on the design stage of the development lifecycle, this article introduces a set of useful strategies and tools for developing secure software. The average "developer-on-the-street," who is not exclusively a developer, is the target group.

4.SYSTEM ARCHITECTURE



5.EXISISTING SYSTEM

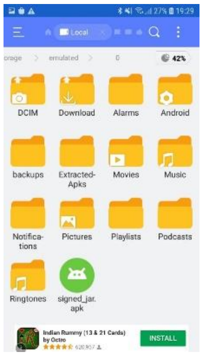
This project focuses on the use of backdoors to hack Android devices and how to prevent this from happening. When installed and activated on the mobile device, the backdoor application enables an attacker to read, write, and modify the data. Backdoor attacks compromise the information security's confidentiality, integrity, and accountability. The meterpreter session is started when the payload is put on the victim's mobile device and the victim launches the program, allowing the attacker to access features including the webcam, contacts, read and send SMS, read and write call logs, access storage, and install applications.

6.PROPOSED SYSTEM

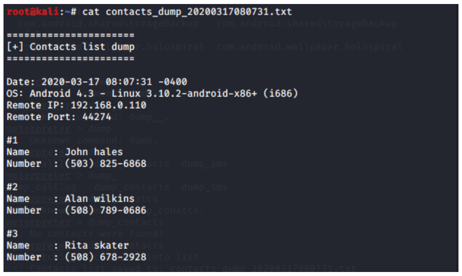
We will incorporate these elements in order to overcome the current model. The attacker can access features like the webcam, contacts, contacts list, contacts list, read SMS, send SMS, read SMS, write SMS, read call log, write call log, access storage, and install applications when the application is installed on the victim's mobile device and the victim opens the application. Binding APK (Embed).

7.GENERATING RESULTS OF TEST

The test findings must include recommendations for how to lessen or get rid of the weaknesses. Here is how a penetration test differs from a security audit. Priority must be given to addressing identified critical vulnerabilities, and a clear timeline must be created to ensure that the vulnerabilities have been fixed. The same penetration testing procedure can be applied to a particular department, network, or system. The cost (and efficacy) of the available remedies, the damage to the firm if the circumstances that caused the vulnerability occur, and the vulnerabilities detected will all influence the solutions that are deployed. One option could be to require a new web server-running system to pass a vulnerability test before the firewall opens the web port.



(a) Installation of apk in android device



```
root@kali:~# cat contacts_dump_20200317080731.txt

=======================
[+] Contacts list dump
=======================

Date: 2020-03-17 08:07:31 -0400
OS: Android 4.3 - Linux 3.10.2-android-x86+ (i686)
Remote IP: 192.168.0.110
Remote Port: 44274

#1
Name    : John hales
Number  : (503) 825-6868

#2
Name    : Alan wilkins
Number  : (508) 789-0686

#3
Name    : Rita skater
Number  : (508) 678-2928
```

(b) Above image shows the Accessed SMS data

8.CONCLUSION

An extensive technique for locating weaknesses in a system is penetration testing. Benefits include preventing financial loss, complying with industry regulations, clients, and shareholders, maintaining the corporate image, and proactive risk removal. Depending on how much information the user has access to, testers can choose between black box, white box, and grey box tests. Depending on the Particular Objectives, testers can choose between internal and external tests. Penetration testing comes in three flavors: network, application, and social engineering. This document provides a basic overview of Android hacking and outlines the method in detail for gaining access to an Android device.

9.REFERENCES

[1]. O. Aslan and R. Samet, "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," 2017 International Conference on Cyberworlds (CW), Chester, pp.222-225, 2017.

[2]. Internet Crime Complaint Centre link: www.ic3.gov.

[3]. H. Gupta and R. Kumar, “Protection against penetration attacks using Metasploit,” in 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, India, pp. 1–4, 2015.

[4]. Muniz, J. & Lakhani, A. (2013). Web Penetration Testing with Kali Linux a practical guide to implementing penetration testing strategies on websites, web applications, and standard web protocols with Kali Linux. Birmingham: Packet Publishing.

[5]. Singh, A. (2012). Metasploit penetration testing cookbook over 70 recipes to master the most widely used penetration testing framework. Birmingham: Packet Pub.

[6]. A. Ghafarian, “Using Kali Linux Security Tools to Create Laboratory Projects for Cybersecurity Education,” in Proceedings of the Future Technologies Conference (FTC) 2018, vol. 881, Cham: Springer International Publishing, pp. 358–367, 2019.

[7]. M. C. Tran and Y. Nakamura, “Classification of HTTP automated software communication behavior using NoSQL database,” in 2016 International Conference on Electronics, Information, and Communications (ICEIC), Danang, Vietnam, pp. 1–4, 2016.

[8]. A. Chowdhury, “Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview,” in Applications and Techniques in Information Security, vol. 651, L. Batten and G. Li, Eds. Singapore: Springer Singapore, pp. 54–65, 2016.

[9]. F. Cuzme-Rodríguez, M. León-Gudiño, L. SuárezZambrano, and M. Domínguez-Limaico, “Offensive Security: Ethical Hacking Methodology on the Web,” in Information and Communication Technologies of Ecuador (TIC.EC), vol. 884,

[10]. M. Botto-Tobar, L. Barba Maggi, J. González-Huerta, P. Villacrés Cevallos, O. S. Gómez, and M. I. Uvidia Fassler, Eds. Cham: Springer International Publishing, pp. 127–140, 2019.

[11]. F. Holik, J. Horalek, O. Marik, S. Neradova and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, pp. 237-242, 2014.

[12]. M. Denis, C. Zena and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, pp. 1-6, 2016.

[13]. S. Nagpure and S. Kurkure, “Vulnerability Assessment and Penetration Testing of Web Application,” in 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), PUNE, India, pp. 1–6, 2017

[14]. L. Qiang, Y. Zeming, L. Baoxu, J. Zhengwei, and Y. Jian, “Framework of Cyber Attack Attribution Based on Threat Intelligence,” in Interoperability, Safety and Security in IoT, vol. 190, N. Mitton, H. Chaouchi, T. Noel, T. Watteyne, A. Gabillon, and P. Capolsini, Eds. Cham: Springer International Publishing, pp. 92–103, 2017.

[15]. Y. Wang and J. Yang, “Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool,” in 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, pp. 110–113, 2017.