Journal of Cyber Health and Computer (JOCHAC)
Volume 1, Issue 1, December 2023
ISSN: 3031- 4623, DOI:10.64163/jochac.v1i1.3

Penetration Testing with OWASP Mobile for Android Security Optimization

Deco Aprilliansyah [1], Imam Riadi [2], Sunardi [3]

[1] Master Program of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia.
[2] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia.
[3] Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia.
Email: [1] deco2007048003@webmail.uad.ac.id
*Corresponding Author

Abstract— Security and privacy are very important on android devices to prevent crimes such as the theft of data and confidential information for users. There are many attack methods that can be carried out by irresponsible parties, one of which is penetration testing. The need to improve the security of android devices from cyber crimes that can occur at any time so that the security and information belonging to users are more secure. Based on this, this study offers how attackers perform penetration testing on targets using android devices using the OWASP Mobile framework based on the steps in the Security Testing Guide (OWASP MSTG) manual. The penetration testing activity is carried out in five steps. Namely, injection of backdoors on the application, finding vulnerabilities, scanning, exploiting and making reports. The results of this study obtained some information on application IOCs and other information in the form of contact data, SMS data, and audio records belonging to the attacked device. Based on this, this research can be used by security parties to patch loopholes in their applications and systems.

Keywords— Android; Penetration Testing; OWASP MSTG; Exploit.

I. INTRODUCTION

The development of smartphone technology is progressing rapidly, and smartphones are used for communication, data exchange, information retrieval, and entertainment, such as video games, online learning, and listening to music[1]-[3]. This makes users dependent on their smartphones. The problem is that this reliance on mobile will never make smartphones free from cybersecurity risks. This development has negative consequences, such as data theft and crime in the form of confidential information for Android device users[4]-[6]. According to Statista, the number of cyberattacks against smartphone users worldwide in December 2021 totaled about 2.2 million attacks[7]. Meanwhile, products from cybersecurity companies detected approximately 3.5 million malicious installation packages on mobile devices in 2021. This is well below the 5.7 million detected the previous year. Note, however, that the numbers recorded in 2021 are about the same as in 2019[8]. One of the most popular smartphone technologies is Android, the mobile operating system [9]. Android is based on the Linux kernel and was developed by Google. As the single most used OS on smartphones globally, Android is in great demand by bad programmers.

Security on the Android operating system is sometimes overlooked by users, such as malware and remote access exploits by third parties. Mobile app security threats are exploding. Bugs and security vulnerabilities in mobile apps can allow hackers to break in and access sensitive information [10]. Communication security and data protection are very important in application development [11]. For this reason, it is necessary to test the security of the application on an Android smartphone.

Testing is essential to do to know how to use android devices safely. This study experimented with doing penetration testing on Android devices using the OWASP Mobile Security Testing Guide to find out security holes.

The penetration tester attack testing system in this test follows the OWASP Mobile Security Testing Guide with five steps: preparation, intelligence gathering, mapping the application, exploitation, and report. This stage aims to obtain information such as Indicators of Compromise (IOCs), Hash Code, activity system files, signature files, SMS data, contacts data, and audio records [12]. This is important because most data is confidential. That's why safety is important. This testing process is expected to help us understand how third-party penetration testing attacks including the OWASP mobile top 10 issues and enable security parties to patch gaps in applications and systems [13].

II. LITERATURE REVIEW

A. Android OS

Android OS is the most pervasive, widespread, and easy-to-use mobile platform. This open-source Linux kernel-based operating system offers greater flexibility due to its customization properties, making it the leading mobile operating system [14]. An Android utility commonly consists of numerous utility components, such

as activities, fragments, services, content material providers, and broadcast receivers [14]. As feature-wealthy Android apps, or apps for short, end up extra not unusual place in safety touchy scenarios, a manner to validate their safety houses is tremendously desirable. Communication security and data protection are very important in application development [11].

B. Penetration Testing on Android OS

Penetration testing is a way to protect your website from attacks by irresponsible individuals and hackers [12]. Importance of identifying issues and gaps to help develop frameworks/tools for designing intrusion-resistant mobile applications by embedding all vulnerabilities at the design stage using the Android Vulnerability Repository [15]. Penetration testing is also carried out with the aim of detecting vulnerabilities, security analysts, and conducting mobile penetration tests using security analysis tools [16].

C. OWASP Mobile Security Testing Guide (MSTG)

OWASP MSTG is a guide for testing mobile application security. it describes technical procedures to verify the requirements listed in MASVS. MSTG includes a list of test cases, each associated with a requirement in MASVS. During MASVS If the requirements are advanced and generic, MSTG will give detailed advice and testing methods based on each mobile OS.

D. Attack Scenarios

This section is an overview of the attack scenarios carried out following the step-by-step OWASP Security Testing Guides in the penetration testing section, and more details can be seen in Fig. 1.

Fig. 1. Attack Scenario AWASP MASTG

It can be seen in Fig. 2. that the steps taken include 5 steps. Namely, the first step of preparation is done by injecting the backdoor and installing the application, the second step of intelligence gathering is done by analyzing vulnerabilities, the third step of mapping the application is made by exploring and scanning application weaknesses, the fourth step of exploitation This is done by sending a command to the target device and remotely accessing the trojan. The fifth step is to send a report on the data obtained from the remote access trojan.

III. RESULT AND DISCUSSION

A. Research Stage

A typical security test is structured as follows:

a. Preparation - Determining the scope of security testing, including the sensitive data, the organization's testing objectives, and any applicable security measures. More broadly, preparation encompasses all client synchronization and legal protection for the tester (often a third party). Keep in mind that attacking a system without express permission is prohibited in many parts of the world.

b. Intelligence Gathering - examining the app's architectural and environmental setting to obtain a broad grasp of the context.

c. Mapping the Application - Based on data from earlier stages, automatic scanning and manual app exploration might be supplemented. A complete understanding of the program, its entry points, the data it contains, and the primary vulnerabilities may be obtained through mapping. The security tester can then prioritize these vulnerabilities by ranking them based on the harm that might result from their exploitation. The development of test cases for potential use during test execution is a part of this phase.

d. Exploitation - In this stage, the security tester attempts to access the app by abusing the flaws found in the earlier step. To ascertain whether vulnerabilities are genuine true positives, this phase is required.

e. Reporting - Security testers report weaknesses during this essential phase for the client. This includes details of the exploitation process, categorization of vulnerability types, documentation of the risk if an attacker compromises the target, and an overview of the data that the tester was able to gain unauthorized access to.

B. Inject Application

At this stage, the tester will enter the payload into the

application, which will later be installed on the victim's device. The backdoor injection process uses the L3mon framework and adjusts to the IP and PORT of the attacker's host. The details can be seen in Fig. 3.

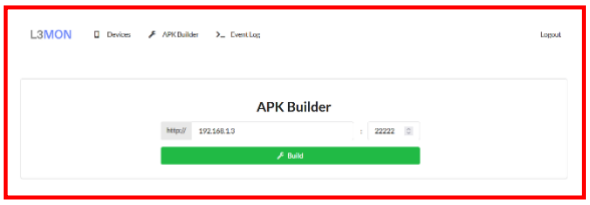

Fig. 2. Injecting application using l3mon

Fig. 3. shows the IP used by the attacker is 192.168.1.3, and the PORT used is 22222. This IP and PORT follow the attacker's HOST, which can be seen in Fig. 4.

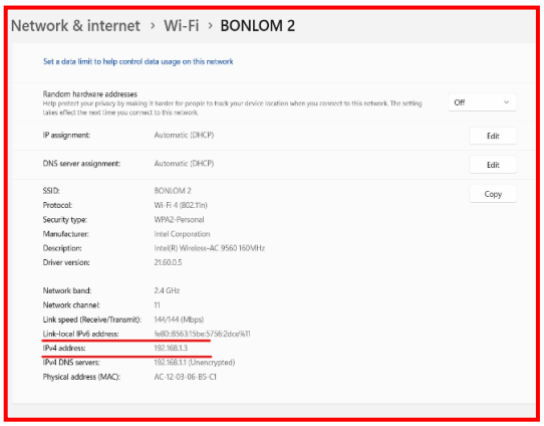

Fig. 3. IP Address attacker

It can be seen in Fig. 4. that the IP Address information on the attacker's device is 192.168.1.3.

C. Intelligence Gathering Application

This stage shows the analysis of the scope of the application that has been injected with the backdoor. Analysis of gathering information can be seen by identifying the permissions requested by the application. The list of permissions on the application can be seen in Fig. 4. It can be seen in Fig. 4. application permission requests in the form of Wake lock, Camera, Write & read external storage, Internet, Access network state, Read SMS, Send SMS, Access wifi state, Read phone state, Read call log, Record Audio, Access location, Read contacts.

Fig. 4. Android manifest application

Malicious applications can use this to send and receive data and other important information by using this permission.

D. Mapping the Application

The results of the manual mapping application found the host entry point contained in the MyReceiver.java file, which can be seen in Fig. 5.

Fig. 5. Display listener settings

Fig. 6. shows the code listener the incoming port used, namely "8088" and "5055".

E.Exploitation Device

The victim's device that has been connected to the attacker's HOST will then be subjected to the Exploitation process, which can be seen in Fig. 6.

Fig. 6. Exploit the device using the attacking host

It can be seen in Fig. 6. that the attacker's IP is 192.168.1.3, and the PORT is 22222. The victim's device will be connected via the IP Address and PORT. Next, the exploitation process will be carried out.

F. Reporting

This stage is a phase where the examiner reports on the attack process and the information that has been obtained during the attack process. The following in Table 1 is some information on the analysis application that has been included in the payload.

Table. 1. IOCs Application

POVERTY	VALUE
MD5	623614337e89113b3ebdc0325bdc0918
SHA1	f7b476070905f35986cdb5764026150d61ab76cb
SHA256	cbea811972b9b87de06eb6c2ea2e291c2981be5fe4c73589352aef4dd0a08f25
Service NAME	com.etechd.l3mon.MainService

Table. 1. shows the information on giving signatures information in the form of hash code md5, sha1, sha256, service name, signature file "rsassa_pkcs1v15," and file type "apk." Based on data, files can be retrieved IOCs SHA-256cbea811972b9b87de06eb6c2ea2e291c2981be5fe4c73589352aef4dd0a08f25.

After successfully exploitation, the attacker managed to get some data between getting contact, Read SMS, and Record audio which can be seen in Fig.s 8.

Fig 8 attacker who managed to get contact

Fig. 8. Shows an attacker who managed to get contact information data from the victim's device. The contact data obtained are *#*#27663368378#*#*, 08080808 (Exploit 1), 22222 (Exploit 2).

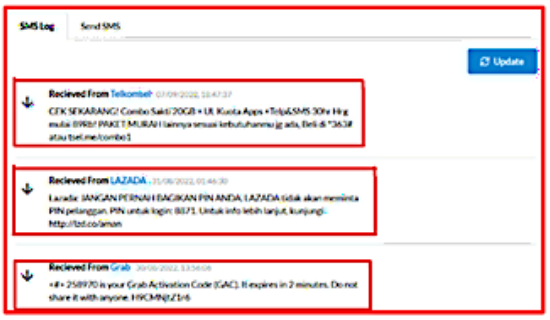

Fig. 9. Dumping data SMS

Fig. 9. shows that the attacker managed to get 3 SMS data from the victim's device.

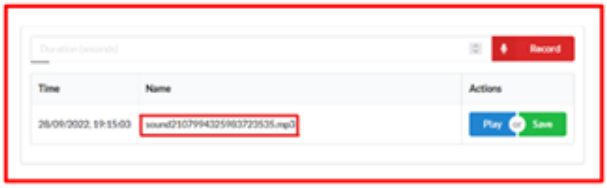

Fig. 10. Record audio from target device

Fig. 10. shows the attacker managed to record audio from the target device. The audio file was recorded on 28/09/22 with the file name "sound2107994325983723535.mp3."

IV. CONCLUSION

Penetration testing on targets using android devices using the OWASP Mobile framework based on the steps in the Security Testing Guide (OWASP MSTG) manual. The penetration testing activity is carried out in five steps. Namely, injection of backdoors on the application, finding vulnerabilities, scanning, exploiting and making reports. The results of this study obtained some information on application IOCs and other information in the form of contact data, SMS data, and audio records belonging to the attacked device. Based on this, this research can be used by security parties to patch loopholes in their applications and systems.

REFERENCE

[1] T. T. Allen, Introduction to discrete event simulation and agent-based modeling: Voting systems, health care, military, and manufacturing, Springer, New York, 2011.

[2] T. T. Ballen, Introducion to discrete event simulation and agent-based modeling: voting systems, health care, military, and manufacturing, 2 ed., Springer, New York, 2011

[3] G. Blanchard and R. Loubere, High-order conservative remapping with a posteriori MOOD stabilization on polygonal meshes, 2015, Available from: http://www.emn.fr/z-info/choco-solver/ [last accessed May 2011].

[4] R. Boggs, J. Bozman, and R. Perry, Reducing downtime and business loss: adressing business risk with effective technology, Tech. Report Technical report 91-18, InternationalData Corporation (IDC), Sernageomin, 2002.

[5] S. Elbaum, A. G. Malishevsky, and G. Rothermel, Test case prioritization: A family of empirical studies, IEEE Trans. Softw. Eng. 28 (Feb. 2002), no. 2, 159–182.

[6] G. Rothermel, A safe efficient regression test selection technique, ACM Trans. Soft. Eng. Methodology 6 (1997), no. 2, 173–210. MR 2000f:91046

[7] G. Rothermel, M. J. Harrold, C. W. Hirt, A. A. Amsden, and J. L. Cook, A safe efficient regression test selection technique, ACM Trans. Soft. Eng. Methodology 6 (1998), no. 2, 173–210.

[8] A. Schulz and G. Doblhammer, Aktueller und Zukünftiger Krankenbestand von Demenz in Deutschland auf Basis der Outinedaten der AOK. (Current and future number of people suffering from dementia in Germany based on routine data from the AOK.), Versorgungs-Report (Piscataway, NJ, USA) (C. Gnster, J. Klose, and N. Schmacke, eds.), IEEE Press, 2012, pp. 161–175.

[9] S. Yoo and M. Harman, Pareto efficient multi-objective test case selection, (Proceedings Of The 2007 International Symposium On Software Testing And Analysis, London, UK), 2007, pp. 140–150.

[10] R. S. Kusuma, "Forensik Serangan Ransomware Ryuk pada Jaringan Cloud", JURNAL MULTIMEDIA NETWORKING INFORMATICS, vol. 9, no. 2, pp. 99–107, Oct. 2023.

[11] K. B. Sarmila and S. V. Manisekaran, "A Study on Security Considerations in IoT Environment and Data Protection Methodologies for Communication in Cloud Computing," *2019 International Carnahan Conference on Security Technology (ICCST)*, Chennai, India, 2019, pp. 1-6, doi: 10.1109/CCST.2019.8888414.

[12] S. -, I. Riadi, and P. Ananda, "Vulnerability Analysis of E-voting Application using Open Web Application Security Project (OWASP) Framework," International Journal of Advanced Computer Science and Applications, vol. 10, no. 11, 2019, doi: 10.14569/ijacsa.2019.0101118.

[13] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, "Mobile Application Security Penetration Testing Based on OWASP," IOP Conference Series: Materials Science and Engineering, vol. 846, no. 1, p. 012036, May 2020, doi: 10.1088/1757-899x/846/1/012036.

[14] R. Ponakala and M. N. Dailey, "LineageOS Android Open Source Mobile Operating System: Strengths And Challenges," Oct. 2020, doi: 10.35543/osf.io/4gch5.

[15] X. Li, L. Yu, and X. P. Luo, "On Discovering Vulnerabilities in Android Applications," Mobile Security and Privacy, pp. 155–166, 2017, doi: 10.1016/b978-0-12-804629-6.00007-9.

[16] "A Process of Penetration Testing Using Various Tools," Mesopotamian Journal of Cyber Security, pp. 94–104, Apr. 2023, doi: 10.58496/mjcs/2023/014.