Vulnerability Assessment and Penetration Testing to Android Device

[1]Minna Elizabath Joshy, [2]Dr. Manjunath M
[1]P.G Student, [2] Assistant Professor,
[1,2]Department of MCA,
[1,2] RV College of Engineering®, Bangalore, India.

Abstract: In today's world where information communication technology has brought the world together, there is increased growth in the areas of the network. Mobile devices are becoming targets for attackers and malicious users due to the increase in their capabilities and usage. Penetration testing is that the process of detecting vulnerabilities of a tool and gaining access to data on the targeted systems to detect vulnerabilities and security issues and proactively protect the system. Vulnerability Assessment and Penetration Testing to android device give access to the remote android mobile phone which is on the same network. The main objective is to assess what an attacker can achieve if they bypass the remote access to a system's security controls, and successfully gain internal access. It is better to search out these vulnerabilities prior to the attackers. The proposed work will assess the security issues that can occur if the exploiter accesses the victim's Android device as it can access all the personal information stored in the device.

IndexTerms **- Vulnerability Assessment, Penetration Testing, Android Debug tool, Metasploit, Android mobile**

I. INTRODUCTION

Cyber security is one of the major issue that we are facing due to excessive growth of networking. As the generation is growing in the technological era and people can be connected with the help of internet, there is a high chance that the devices which use internet becomes vulnerable [9][10]. The easiest and efficient way for people to get connected through network is by using their smartphones. The studies have shown that smartphones are not only used for communication or social networking but also online payment and many depend on smartphones for their daily online transactions. Hence, mobile devices are becoming the target for the attackers or the malicious users. The use of smartphones increases and the version is growing unexpectedly because of their wealth and versatile functionality. The versatility and comfort of those gadgets took them in advance from different comparable gadgets. Currently, Android is one of the maximum popular open-source operating systems for Smartphones. The fast boom and version of the mobile device make it extra appealing for hackers.

Mobile device and its applications play an important role in modern generation. Smartphone growth and adaptation is increasing rapidly because of their rich and versatile functionality. The adaptability and comfort of those gadgets took them an ahead from other comparative gadgets. We not just utilize the applications for countless purposes on our cell phones yet in addition send the applications to different kinds of keen gadgets. The multi-stage organization of uses is, uncommonly, valid for applications that are intended to run on the Android OS, since Android is that the most famous OS for mobile gadgets. These applications are often very critical in nature like mobile banking, and mobile payment systems and users are often unknowing about the safety risks involved in such applications [3].

Mobile applications play an ever-greater essential position in present day society. The multi-platform deployment of programs is, in particular, actual for programs which might be designed to run at the Android operating system, due to the fact Android is the most famous operating system for smart devices. Although the significance of cellular applications grows each day, the latest vulnerability reviews argue the deficiency of applications to fulfil current safety standards. Testing techniques alleviate the trouble by figuring out safety violations in software program implementations.

Mobile gadgets have become objectives for hackers and malicious users because of the multi fold boom in their competencies and usage. Security threats are greater distinguished in mobile banking applications. As those mobile banking applications, store, transmit and get entry to sensitive and confidential information, so utmost precedence must receive to steady mobile banking applications. Security stays one of the main issues of information systems. The developing connectivity of computer systems via the Internet, the growing extensibility, and the unbridled boom of the scale and complexity of systems have made gadget protection a larger hassle now than in within the past.

The proposed research of vulnerability analysis and penetration testing focused on exploiting the android smartphones. The objective of this work is gets to know about what the exploiter can achieve if they remotely access the Android device and gain the internal control. Vulnerability Assessment and Penetration Testing to android device give access to the remote android mobile phone which is on the same network. The proposed work will assess the security issues that can occur if the exploiter accesses the victim's android device as it can access all the personal information stored in the device.

The heart of all android architecture is the Linux kernel which is responsible for drivers like memory management, camera drivers, keypad, etc. Hence through any Linux operating system, basic attacking to an android device can be done. All android phone has the option of being a developer. Through enabling the developer option makes it easy for the attackers to bypass into android system.

II. VULNERABILITY ASSESSMENT AND PENETRATION TESTING

A vulnerability assessment is done to check the weakness and security problems of a device. That means, to know how safe and secure the device is to use. The vulnerability assessment can be done through penetration testing [6]. Penetration testing is the process of performing the test on the device by checking the network and finding ways to exploit the device to be tested [9]. With the help of penetration testing the faults can be found out and make the developers aware of the issue, and henceforth find a solution to cover up the problem.

Vulnerabilities are the defects that can cause problems in system security [8]. Henceforth the devices have to be tested prior, to avoid falling into trouble from leakage of personal information which is securely stored in our android devices. The personal information can be anything which includes the bank details as the bank related messages can be viewed, then other confidential documents, pictures, etc. that are stored in our system can be pulled by the exploiter.

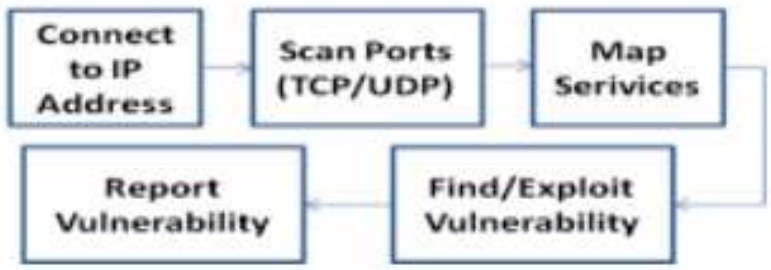

Figure 1: VAPT Process [2]

The entire technique of VAPT is performed in 2 main parts. The first element offers with the Analysis and Discovery of present Vulnerabilities, which can also additionally end in numerous Cyber threat. The second element offers the Exploitation of the discovered set of Vulnerabilities, to choose their seriousness and effect over the Target system.

- Test network or device uses the tools and strategies that intruders use.
- It can demonstrate at what intensity the vulnerabilities can be exploited.
- The vulnerabilities are validated.

Penetration testing is very vital and it guarantees that the organization's network is secure and updated in meeting safety standards. So via way of means of escaping, to carry out penetration check-in systems is making an attempt to leverage the vulnerabilities observed, therefore there's no manner of understanding the dangers which can be provided to network system based on the one's vulnerabilities.

III. METHODOLOGY USED IN VAPT

The project Penetration Testing and Vulnerability Assessment of Remote System check the vulnerability which will happen in android mobile when connected to same network. A penetration test, occasionally called pentest, may be a method of evaluating the safety of a distant system or network by simulating an attack from a malicious source, referred to as a Cracker. Alongside penetration testing, a general overview about the Android security mechanism is described to supply the reader an idea of how it works. Vulnerability assessment gives vague evaluation of issues by testing for vulnerabilities done through penetrating barriers is beneficial adjunct.

The Android Smartphone has become mainstream in light of its quickly expanding applications identified with gaming, instruction, business, banking, and informal organizations. Hence the Smartphone store has different sort of information in their database like personnel, banking account and knowledge associated with businesses and therefore the security is critical issue for Smartphone against above stated information. As the android is an open source of applications which are developing very rapidly and since of these open source applications the hackers can easily target the Smartphone.

The proposed work is often through with help of ADB (Android Debug Bridge) tool or Metasploit Framework, which contains an inbuilt tool for developing and executing exploit code against a foreign target machine. ADB tool are often installed in any Linux system. From the proposed work it's identified that when an android device is connected to an equivalent network and once through USB cable if it's connected to the attacker system, then it's easy to urge all the knowledge and may control the victim's phone [2].

Once the exploiter or the attacker cracks into the android device, the device can be handled completely by the attacker without the user's knowledge. Then the exploiter can retrieve the data from the android device and can save it in the attacker's system for later use or for exploiting. Once the attacker accessed the device, it is possible to remove the files from the victim's phone without the knowledge of the user. Even the live update of what the victim does can be viewed and recorded to the exploiter's system. The exploiter will be able to control the android smartphones from the system used for exploiting.

The attacker can get the screen copy of the android phone in an android emulator. When the device is opened in an emulator view, the attacker can easily check the information because the emulator displays the copy of our phone on the exploiter's system screen. By using the system keyboard and cursor, the victim's device can operate.

IV. Proposed system

The purpose of the proposed research is to evaluate the security and identify problems in the mobile devices. The Penetration Testing and Vulnerability Assessment of Remote System provides access to the victim's device, identify the vulnerability through penetration testing. The complexity of systems is growing day through day. This ends in an increasing number of vulnerabilities in Systems. Attackers use those vulnerabilities to take advantage of the victim's system.

Vulnerability evaluation is the procedure of scanning the gadget or software program or a network to discover the weak spot and loophole in that. These loopholes can offer a backdoor to the attacker to assault the victim. A device might also additionally have got right of entry to manage vulnerability, Boundary circumstance vulnerability. Penetration testing is the procedure of detecting gadget vulnerabilities and gaining entry to and records on centered systems intending to locate vulnerabilities and protection troubles and proactively shield the device.

Functional Requirement

The intruder's and the victim's device should have proper network connection. Both the device should be connected to same network. The network interruption will not give access to the device as it is keep on getting connected and disconnected to same network as well as different. Hence to get the correct outcome network connectivity is important.

- The exploiter will exploit the remote Android device connected to the same network as the exploiter.
- If the attacker wants attacks using the ADB tool, then the developer option in the android phone has to be enabled.
- The main requirement for cracking a device with an ADB tool is once the device should be connected using a USB cable to the system through which it is exploited.
- The victim's phone can be completely controlled by the exploiter even if the device is having a password lock.

Non Functional Requirement

- Reliability: The outcome of the project is cracking into an android device which is connected in the same network. The victim's and exploiter's system should be under same network connection.
- Security: The project show case all the security issues that can happen if an android device is exploited. That is, what all the intruder can access from the mobile phone like contacts can be viewed, mails, photos can be accessed, etc.
- Safety: Through the execution of Penetration Testing and Vulnerability Assessment of remote system, it is understood that how unsafe our android device is, when connected with same network.

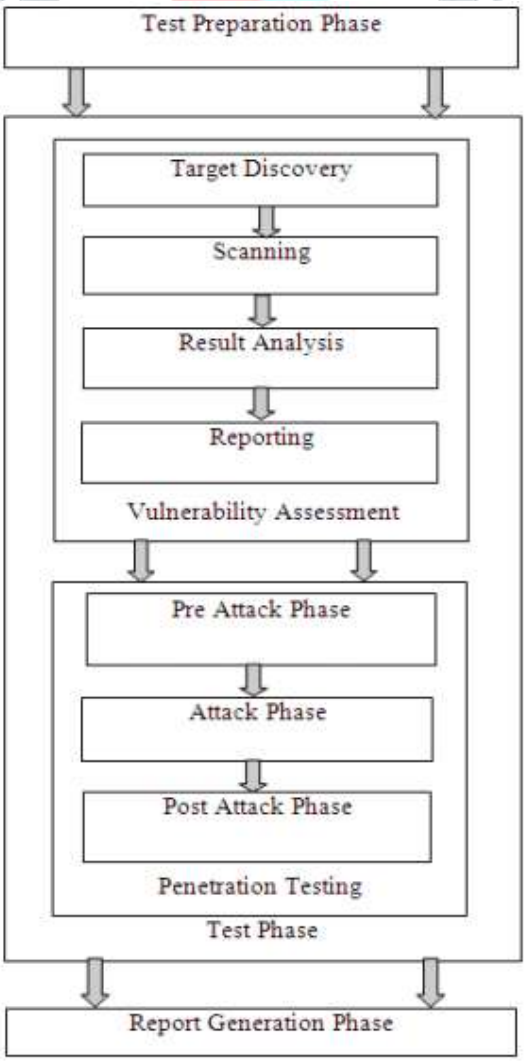

Figure 2: Phases of VAPT [9]

From figure 4.1, the test preparation phase has got mainly two blocks, vulnerability assessment and test phase or penetration testing phase.

In the vulnerability assessment phase, first the victim or the target has to be identified to perform the vulnerability check. Once the target device is identified, find out all the flaws that are found by cracking into the device, so that the problems of the device can be identified. Hence, in the vulnerability assessment phase, the issues are identified.

The identified issues are tested in the penetration testing to identify how intense the issues are. The pre attack phase is the phase before the attack happens. In the attack phase, the exploiter will get into the victim device and exploit the device by accessing the data from the android mobile phone. The post-attack phase means the device after the exploitation happened. That is all the confidential or private data is accesses and saved by the exploiter for using it later or when the exploiter needs it.

V. CONCLUSION

The proposed research focussed on android phone devices as the number of users using the android smartphone is more. As mobile platform is growing the attackers or malicious users targets on these devices to be exploited [3]. Vulnerability Assessment and Penetration Testing is a better to check out the problems and makes the user aware about the issues or problems that can happen. VAPT helps in identifying the security issues and to safeguard the users from falling into troubles [1].

As networking is growing very fast, the vulnerability of the systems is also increasing and more security issues are happening. Penetration testing or pen testing is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. The main objective of penetration test is to assess what an attacker can achieve if they bypass the remote access to a systems security controls and successfully gain internal access. It is better to find out these vulnerabilities in advance before attacker does.

REFERENCES

[1] F. Palma, N. Realista, C. Serrão, L. Nunes, J. Oliveira and A. Almeida, "Automated security testing of Android applications for secure mobile development," 2020 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Porto, Portugal, 2020, pp. 222-231, doi: 10.1109/ICSTW50294.2020.00046.

[2] Y. Khera, D. Kumar, Sujay and N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 525-530, doi: 10.1109/COMITCon.2019.8862224.

[3] W. van der Lee and S. Verwer, "Vulnerability Detection on Mobile Applications Using State Machine Inference," 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 1-10, doi: 10.1109/EuroSPW.2018.00008.

[4] Nagpure, S., & Kurkure, S. (2018). Vulnerability Assessment and Penetration Testing of Web Application. 2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017, 1–6.

[5] S. Bojjagani and V. N. Sastry, "VAPTAi: A Threat Model for Vulnerability Assessment and Penetration Testing of Android and iOS Mobile Banking Apps," 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC), San Jose, CA, USA, 2017, pp. 77-86, doi: 10.1109/CIC.2017.00022.

[6] Shinde, P. S., & Ardhapurkar, S. B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. *IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare*.

[7] Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, *11*(1), 27–49.

[8] Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, *57*, 710–715.

[9] Shah, S., & Mehtre, B. M. (2013). A Latest Approach to Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing. *International Journal of Electronics Communication and Computer Engineering*, *4*(6), 47–52.

[10] Sachin Umrao, M. K. (2011). *For Vulnerability Assessment And Penetration Testing*. (January 2012), 1–20.