A Collaborative Approach for Android Hacking by Integrating Evil-Droid, Ngrok, Armitage and its Countermeasures

Reshma Sajeev
Department Of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally, India
reshmasajeev@mca.ajce.in

Sinimol Joseph
Department Of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally, India
sinimoljoseph@mca.ajce.in

Sivanand Biju
Department Of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally, India
sivanandbiju@mca.ajce.in

Merin Manoj
Department Of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally, India
merinmanoj@amaljyothi.ac.in

***Abstract*—Android is the most commonly used operating system which is designed for touchscreen mobile devices. Security is an important feature in the android platform. We can manipulate or gain unauthorized access such as intercepting telephone calls or accessing voicemail messages from Android devices by using penetration testing tools, it is known as Android hacking. Kali Linux mainly aims at security auditing and penetration testing. Penetration testing tools are used for testing security vulnerabilities in computer systems, web applications and networks that an attacker could exploit.**

Evil-Droid is a penetration testing tool used for generating and embedding apk payloads in Android platforms. The penetration testing is used to identify the weak spots in Android's security posture and to measure the compliance of its security policy. Armitage is a graphical cyber attack management tool and Ngrok is a tool used for securing introspectable tunnels to localhost webhook development. In this paper, we discuss the integration of these three tools and the countermeasures to prevent Android devices from attacks. By this integration attackers can penetrate android platforms over the internet by using a GUI.

Keywords—Penetration testing, Android hacking, Payload, Evil-Droid, Ngrok, Armitage, GUI, TCP, LHOST, LPORT

I. Introduction

Nowadays, Mobile developers most commonly use Android OS to develop smartphones because of its performance, features, and services. Smartphones provide vast services such as phone calls, internet services, online and offline games, email, video calls, social networking apps, messaging, storing and sharing files, etc. So it is necessary to ensure security and safety in android devices. The android developer provides security in the form of authentication mechanisms such as passcode, pattern, fingerprint or face detection. Even though some built-in safety features are present in Android devices to prevent viruses and malware, they are less secure.

As the use of android devices is increasing day-by-day, the built-in security needs to be high. New versions of Android OS provide new kinds of integrated security models. However, many techniques can be used to penetrate the wall of security in Android. One such technique is the integrated framework of Evil-Droid, Ngrok, and Armitage. Armitage could be a penetration testing collaboration tool for visualizing targets, recommending exploits, and exposes the advanced post-exploitation options inside the framework. Armitage is a graphical interface for the Metasploit Framework.

The Android developers are using Kali Linux pen testing tools to exploit vulnerabilities, but these tools have some limitations. This integrated framework of Evil-Droid, Ngrok and Armitage can overcome those limitations.

II. Literature Review

Khulood Al Zaadi (2016) is talk about tricks used in Android device hacking and how to prevent these attacks to provide security for personal data and information.The users needs to be co-operate with both Android device companies and third party Applications (i.e. WhatsApp) in identifying any noticeable and critical vulnerabilities. Tricks used in

Android device hacking and how to prevent these attacks to provide security for personal data and information.

Jorja Wright et al. (2012) [2] talks regarding the requirement for antivirus applications and secure lock to guard sensitive and private information in smartphones. An ancient security package found in personal computers,like firewalls, antivirus, and cryptography, isn't presently on the market in smartphones. Moreover, smartphones area units are even additional vulnerable than personal computers as a result of additional folks area unit exploitation smartphones to undertake to do to try to to personal tasks.Nowadays, smartphone users will email, use social networking applications (Facebook and Twitter), purchase and transfer varied applications and look. What is more, users will currently conduct financial transactions,like shopping for product, redeeming coupons and tickets, banking and process location payments.Monetary transactions area unit particularly enticing to cyber attackers as a result of they're going to gain access to bank account data when hacking a user's smartphone.

Haya and Sanaa (2018) describes the broad adoption of smartphones has outdated the desktop computers and laptops as a primary computing platform, because of quality, constant property and application diversity. Mobile devices comprehend storage of thorough data together with sensitive ones like authentication credentials, pictures, videos, personal information, work data, and far additional. Thus, securing information kept on mobile devices becomes a vital issue. During this review, we have a tendency to investigate the security of robot storage models between 2013 and 2018. many threats square measure found among the literature which is able to be categorised as physical or software system threats. to boot, the prevailing solutions for each class square measure highlighted. Though robots provide valuable coding systems together with full disk coding and keychain to bolster the data storage security, the coding key, that is kept among the device, remains at risk of physical threats.

Jalal and Jawwad (2017) is organizing the protection challenges of robots in numerous sections. The primary section discusses the robot security design during which summaries permission mechanism, sandboxing, access management and additionally outline the elements encapsulation and application language and Second section discuss Vulnerabilities in robot Smartphone like net read, SSL/TLS and NFC. It additionally highlights vulnerability relating to social and sharing authentication flaws. Third section is concerning the protection challenges wherever we have a tendency to discuss the various threats to robots thanks to the actual fact that doable attacks compromised the protection of robot smartphones rather like privilege step-up attack, communication attack, privacy connected attack. Smartphones use open houses for communication that arisen several security challenges.

Karthik and Sumitra (2017) give the notice regarding humanoid OS permission-based models. that permits humanoid applications to access user data, system data,device data and external resources of Smartphones. The developer should declare the permissions for the humanoid application. The user should settle for these permissions for productive installation of Associate in Nursing humanoid application. These permissions square measure declarations. At the time of installation, if the permissions square measure allowed by the user, the app will access resources and information anytime. It doesn't want re-request for permissions once more. humanoid OS is susceptible to numerous security attacks because of its weakness in security. This paper tells regarding the misuse of app permissions exploitation Shared User ID, however two-factor authentications fail because of inappropriate and improper usage of app permissions exploitation spyware, knowledge thieving in humanoid applications, security breaches or attacks in humanoid and analysis of humanoid, iOS and Windows OS concerning its security

Zheran et al., (2014), robot security has been a hot spot recently in each tutorial analysis and public problems as a result of varied instances of security attacks and privacy run on robot platforms. robot security has been designed upon a permission primarily based mechanism that restricts accesses of third-party robot applications to vital resources on academic degree robot device.throughout this paper, we've got a bent to tend to investigate the arising problems in robot security, in conjunction with coarse roughness of permissions, incompetent permission administration, meagerly permission documentation, over-claim of permissions, permission modification of magnitude attack, and Time of Check to Time of Use(TOCTOU) attack. we've got a bent to tend perhaps the relationships among these problems, and investigate the prevailing countermeasures to want care of these problems. Specifically, we provide a scientific review on the event of these countermeasures, and compare them per their technical decisions. Finally, we've got a bent to propose some ways to mitigate the danger in robot security.

Bahman et al., (2016) demonstrate the technique to assist inexperienced users to form the proper permission granting selections.In current mechanism style vogue, users have to be compelled to decide whether or not or not Associate in Nursing app is safe to use or not. knowledgeable users can build savvy selections to forestall spare privacy breach. However, inexperienced users might not be able to decide properly. to assist inexperienced users to create a right permission granting selections, we've got an inclination to propose RecDroid. RecDroid could even be a crowd sourcing recommendation framework that facilitates a user-help-user atmosphere concerning smartphone

permission management.In this framework, the responses from knowledgeable users are mass and urged to different users. We've got an inclination to implement our model on the mechanism platform and evaluated the system through simulation and real user study.

Ali et al., (2017) propose AndroDialysis2, a system that analyzes 2 differing types of Intent objects, i.e., implicit and express Intents. to gauge the effectiveness of the projected system, we'll compare our results with that from a base-line detection system that uses similar level of coarseness, which we are going to then analyze the permissions usage. The effectiveness of humanoid Intents (explicit and implicit) as a distinctive feature for distinguishing malicious applications.

III. METHODOLOGY:

We can use Kali Linux OS with a high-speed internet connection to easily exploit the insecurities in Android devices. We can clone the Evil-Droid from GitHub, the Ngrok for Linux OS can be downloaded from the website https://ngrok.com/download and the tool Armitage is already built-in Kali OS. We can establish a secure tunnel from a public endpoint such as the internet by using Ngrok. Evil-Droid is used to create the apk payload and the Armitage GUI can be used to exploit the vulnerabilities of target devices which have the payload.

Integrated working of Ngrok, Evil-Droid and Armitage:

STEP 1:

Download or clone Evil-Droid from GitHub
kali> git clone https://github.com/M4sc3r4no/Evil-Droid.git

STEP 2:

Go to the website https://ngrok.com/download and create an account for sign in.

STEP 3:

Download the client library appropriate for the OS used.

STEP 4:

Unzip the Ngrok library by using the command.

kali> unzip /path/to/ngrok.zip

STEP 5:

Set the auth token to the Ngrok configuration file.

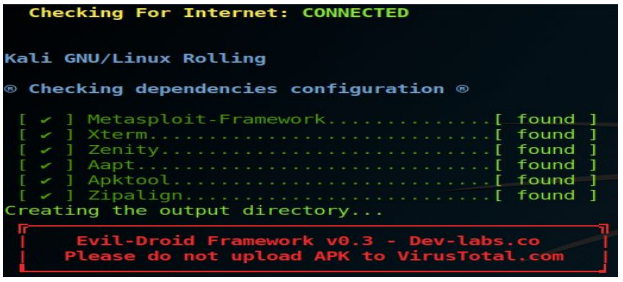
kali>./ngrok authtoken <your token here>

STEP 6:

Execute Evil-Droid

kali> ./evil-droid

After executing the above command we can see the following window



STEP 7:

Give permission to execute the framework

STEP 8:

Select the backdoor option from the menu

We have 5 different options:

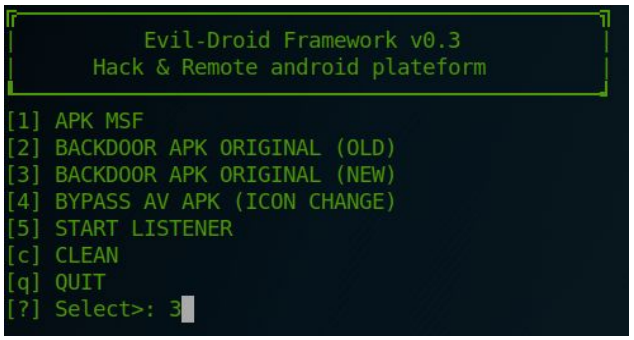
option **1**: This option is used to create a malicious apk payload

option **2**: Here we use the Backdoor-apk shell script to add a backdoor to an existing android apk file

option **3**: Here we use the Backdoor-apk shell script to add a backdoor to an existing android apk file and it creates a new apk file

option **4**: Here we can create a malicious apk file and that can bypass the antivirus

option **5**: It is used to attack an android device which already have the payload



STEP 9:

Create a tunnel for Ngrok by using the protocol and port number

kali> ./ngrok tcp 443

After executing the command the Ngrok provides a Local HOST IP address and Listening PORT number to make the android attack over the internet. It will be used in Evil-Droid to the creation of payload and in Armitage to listen to the target device to perform penetration testing.

STEP 10:

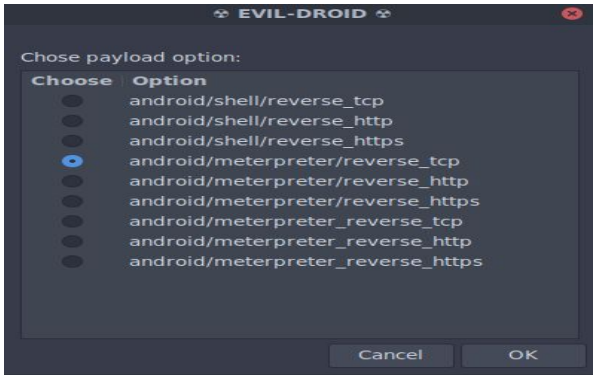
Set the IP address and port number that is provided by Ngrok.

STEP 11:

Give a name to your apk file

STEP 12:

Select the listener as android/meterpreter/reverse_tcp



STEP 13:

The framework generates and stores the payload in its directory.

STEP 14:

Select the multi handler option to make the connection

STEP 15:

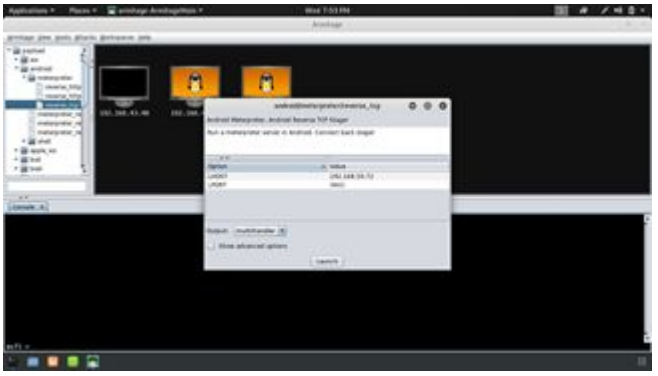
Send the generated apk file to the targeted device and attack the target using the Armitage GUI.

STEP 16:

Start Armitage to attack target device with GUI.

STEP 17:

Running Armitage and attacker setup**:**
When the victim successfully installed the apk, the attacker will find a listener on the attacker machine. do this by using the following step.
payload > android > meterpreter > reverse_tcp
After that a multi/handler window will appear. Then the attacker needs to set the LPORT for communication.

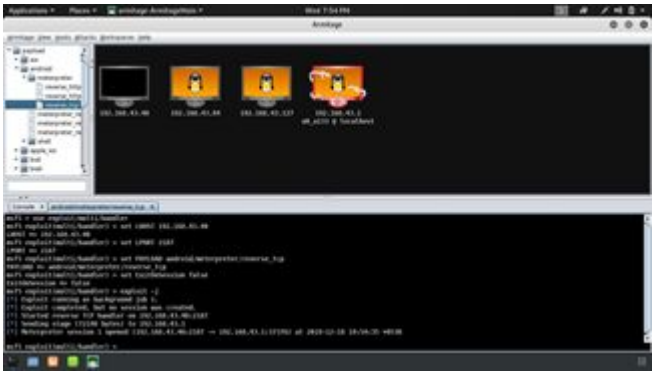


STEP 18:

Start listening:

Once the victim installed and opened the apk payload on their device it will create a remote session with the attacker's machine. The target machine on Armitage turns red with a lightning effect. After that the attacker opens a meterpreter prompt by right-clicking on the host by the following step.

Meterpreter > Interact > Meterpreter Shell



STEP 19:

Accessing files on victims device:
Accessing files on the victim's device by following step. meterpreter > Explore > Browse files We can download the files from the victim's device.

We can use the command-line interface to attack, some of the basic commands and its uses are given below:

- webcam_snap - Take a snapshot
- webcam_stream - Play a video stream
- webcam_list - List the camera types in the device
- record_mic - Record audio from victim's phone using mic.
- sysinfo - Get information about the target device.
- localtime - Get the local time
- activity_start - Start an activity on a victim's device.
- download - Download files from the target device
- dump_contacts - View the contact details
- dump_sms - Retrieve messages from the victim's phone.
- send_sms - Send message from victims number to another number
- set_audio_mode - Set the android device mode in silent to ringing
- dump_calllog - View the call history details

IV. Disadvantages:

Not every aspect of penetration testing tools is completely good by its definition.

- Penetration testers have limitations on the environment of testing
- The integrated pen test tool Evil-Droid needs a high-speed data connection to attack the Android device
- While using the Metasploit framework it creates sessions to perform hacking, the demerit is that the sessions are closed instantly without any warning
- These pen test tools can be used by professionals or amateur hackers to collect sensitive data of a person or an organization
- To exploit vulnerabilities the periodical interaction with the malicious software is essential
- Evil-Droid cannot perform attack over Wide Area Network
- The Metasploit is widely used in a different type of pen-testing tools, it only supports command-line interface in Android device

V. Advantages:

The Evil-Droid, Ngrok, and Armitage are taken into account as penetration testing tools in the Kali Linux system. Penetration testing and vulnerability scanning are completely different techniques, a vulnerability scan is employed to spot and report vulnerabilities whereas penetration testing is employed to take advantage of vulnerabilities or otherwise defeat the safety controls of a system. Penetration testing is a licensed proactive effort to assess the safety of an IT infrastructure by rigorously running tests to take advantage of vulnerabilities of the system. These evaluations help to verify the effectiveness of defensive mechanisms and adherence of end-users to security procedures. The benefits of pen test tools are given below:

- Detect and arrange security threats
- By the integration of Ngrok with Evil-Droid provide the attack of the target device in different network
- Any company, corporation, or organization that ought to have their system security checked often by pen test tools and update their security measures to prevent the negative impact of system time period and felonious hacking
- In case of an organization, these tools are used to avoid the expense of service disturbances and security breaches
- The Armitage in this integrated framework provides a user-friendly GUI to test the device.
- The integrated tools can be used to create malicious code injected apk files in 2 or 3 minutes.
- The usage and working with commands in Metasploit are very easy
- It can be used for academic purposes
- Can check out the latest software security
- By the use of the integrated tools, we can measure the level of security in a device
- These tools have a high scope in case of cybercrimes.

VI. Counter measures to ensure security in Android devices:

Every bit of wise information fits within the smartphone thus every mobile device may be a social network hub, information storage, photo gallery and a recorder of sound and video. All of those functions build our mobile devices extraordinarily enticing targets for malicious actors. Thus defensive against the wide selection of mobile threats is required. The Android developers have to develop their OS with the flexibility to trace and destroy the insecurities. The user has to bear in mind regarding the vulnerabilities of smartphones, the kind of offensive tools and ways to forestall attacks. We can avoid these sorts of attacks by utilizing security measures in Android devices. Some of the safety measures are given:

- Only purchase smartphones from vendors who issue security patches for android
- Update the operating system regularly
- Do not save all passwords
- Use two-factor authentication
- Take benefits of inbuilt android safety features
- Do not open suspicious SMS

- Make sure your wireless fidelity network is secure (and take care with public WiFi)
- Use the antivirus app
- Do not click on suspicious emails
- Backup android phone's data
- Install apps solely from verified developers
- Encrypt the information keep in android device
- Make right permission granting decisions to third party applications

VII. Conclusion:

Android devices are handheld devices that are used for multiple functionalities and it also contains a lot of third party applications. These applications can have a wide range of vulnerabilities. By using this, an attacker can get access to the Android device and can take control of the whole device without the knowledge of the user. So before deployment of the device, the developers need to find out the vulnerabilities and ensure security to prevent these types of malware from smartphones. For this, they can use penetration testing tools.

In this work we discuss the importance of security in Android devices, need for pen testing and the integrated working of Evil-Droid, Ngrok, and Armitage in ethical hacking. Advantages and disadvantages of the pen testing tools and the countermeasures to ensure security in android devices are mentioned to make people aware about security breaches.

References

[1] Khulood Al Zaadi, "Android Device Hacking Tricks and Countermeasures", (2016), College of Technological Innovation, Zayed University.

[2] Jorja Wrightn (a),Maurice E. Dawson J (b), Marwan Omar (c) "Cyber Security and Mobile Threats: The Need For Antivirus Applications For Smartphones",(2012), Florida Institute of Technology (a), USA, Alabama A&M University USA (b) , Colorado Technical University, USA (c).

[3] Haya Altuwaijri, Sanaa Ghouzali, "Android data storage security: A review", (2018), Department of Information Technology, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

[4] Jalal Bhayo Hur (a) , Jawwad Shamsi (b) , "A survey on security issues, vulnerabilities and attacks in Android based smartphone", (2017), (a) National University of Computer and Emerging Science Islamabad, (b) National University of Computer and Emerging Sciences, Karachi, Pakistan.

[5] Karthick Sowndarajan, Sumitra Binu,"Android security issues and solutions", (2017), Christ University, Bangalore

[6] Zheran Fang (a),Weili Han (a), Yingjiu Li (c), "Permission based Android security: Issues and countermeasures", (2014), (a) Software School, Fudan University , Shanghai, 201203, China, (b) School of Information Systems, Singapore Management University, Singapore.

[7] Bahman Rashidi (a), Carol Fung (a), Tam Vu,"Android fine-grained permission control system with real-time expert recommendations", (2016), 1 & 2 Virginia Commonwealth University, Richmond, VA 23284-3068, USA, 3 University of Colorado Denver, Denver, CO 80217-3364, US

[8] 1 Ali Feizollah, 2 Nor BadrulAnuar, 3 RosliSalleh, 4 GuillermoSuarez-Tangil, 5 StevenFurnellc,"AndroDialysis: Analysis of Android Intent Effectiveness in Malware Detection", (2017), 1,2 & 3 Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia, 4 Computer Security (COSEC) Lab, Department of Computer Science, Universidad Carlos III de Madrid, 28911 Leganes, Madrid, Spain, 5 Centre for Security, Communications and Network Research, School of Computing, Electronics and arithmetic, Plymouth University, Drake Circus, Plymouth PL4 8AA, UK