INTERNATIONAL JOURNAL OF EMERGING TECHNOLOGIES IN ENGINEERING
Volume 1,Issue 1,May 2026

ANDROID HACKING AND EXPLOITATION USING KALI LINUX : A CYBER FORENSIC ANALYSIS OF VULNERABIILTIES AND MITIGATION

[1] G.Vishvanath Sundharam, [2] Sudhakaran S , [3] Vijayasarathi S, [4] James Godwin G.

[1] Assistant Professor, Department of CSE(Cyber Security),Muthayammal Engineering College,

[2,3,4] Student of CSE(Cyber Security), Muthayammal Engineering College.

[1] sudhakartechw@gmail.com, [2] vpvijayasarathi15@gmail.com

ABSTRACT

IT security is a paramount concern in today's internet landscape due to the prevalence of communication activities. Testing for personal data theft using social engineering methods aims to identify potential security vulnerabilities in the system and network of a user's Android device. These vulnerabilities could be exploited by hackers if users are unaware of social engineering tactics, allowing for data theft through the use of a Remote Administration Tool (RAT) inadvertently downloaded onto the Android device. The deployment of a RAT via social engineering represents a viable and effective method for compromising the privacy of Android users. This study provides an overview of fundamental concepts related to data theft, ranging from recent call and personal data breaches to the remote manipulation of Android users' cameras and microphones. users no longer need to install additional tools manually. Apart from that, Kali Linux also has an intuitive user interface so that users can efficiently operate the system and the tools provided. Another advantage is modifying and customizing the tools according to user needs through manual configuration or built-in features such as meta packages. Thus, Kali Linux is one of the right choices for android hacking practitioners in conducting security testing on the Android system.

Keywords : RAT ISO USB APK NAMP FAT32

INTRODUCTION

One of the most significant inventions in human history that have changed how we do things is the Internet. The Internet has changed how we communicate, do business, and interact with each other. Today, people no longer have to wait to hear from someone because they can communicate easily through the Internet. The Internet has also enabled businesses and individuals to receive payments instantly and track their fleets and cargo. Security and information technology are increasingly important to society and the ICT industry in this modern era. Security experts have developed various high-performance security tools to ensure that information on the Internet remains safe and not vulnerable to attack. Various techniques, such as Layered Design, Assurance or Proof of Correctness, Software Engineering Environment, and Penetration

Testing, test a complete, integrated, and reliable software, hardware, and people operational computer base.

One example is using open-source frameworks such as Metasploit for exploit creation and penetration testing, which comes with over 1,600 exploits and 495 payloads to attack computer networks and systems. No matter how strong an Android's security system is, it can still be penetrated if the user is still easy to manipulate, especially using social engineering methods. Social engineering is a manipulation technique that exploits human error to access private information or valuable data. In the world of cybercrime, this type of human hacking scam can lure unsuspecting users. The most common is manipulating Android users to install an application, possibly under the guise of an e-ticket,

package delivery receipt numbers for tracking, or other deceptive applications, where these applications are remote administration tools used for personal data theft. Remote addressing tools android hacking is a technology that allows someone to remotely access an Android device without having to be near the device. Hackers use remote addressing tools to exploit vulnerabilities or loopholes in the Android security system to access the device and gain access to sensitive data such as photos, text messages, or financial information.

LITERATURE REVIEW

Title : Android mobile hacking using Linux

Authors : Arulpradeep S. P, Vinothkumar P, Nilavarasan G. S

Concept : Backdoors are one of the most complicated types of Android malware. A normal backdoor carries out its functionalities such as installing itself into the system directory, disabling system apps, or gaining access to app's data, to steal and upload sensitive info, download and ask to install applications and set up mobile when setting proper Android permissions.

This project focus on how Android devices are hacked using backdoors and how they can be stopped from doing so. The backdoor application when installed and turned on the mobile allows an attacker to read, write and modify the data. Due to Backdoor attacks Confidentiality, Integrity, and Accountability of the information security are lost.

Limitations

This research paper provides a complete survey of current research results under web application security. We have covered all properties of web application development, understood the important security functions and properties that secure web applications should use and divided existing works into three major classes .we also discuss a few issues that still need to be considered.

References :

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

[2]. 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

[3]. 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.

[4]. 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, M.BottoTobar, L. BarbaMaggi, J. González-Huerta, P. VillacrésCevallos, O. S. Gómez, and M. I. UvidiaFassler, Eds. Cham: Springer International Publishing, pp. 127–140, 2019.

[5]. 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.

Title : Android Hacking in Kali Linux Using Metasploit Framework

Authors : Abhishek Arote , Umakant Mandawkar

Concept : IT Security is a major concern of the internet as almost all communication takes place over the internet today. The purpose of penetration testing is to ensure that the system and network do not have a security breach that could allow unauthorized access to the system and network. A possible and appropriate way to prevent system and network hacking is penetration testing. The document outlines some basic concepts of penetration testing, evaluating existing tools and exploits, and using the Metasploit framework for penetration testing and running exploits within the framework and tools

Limitations : The limitations of penetration testing in IT security stem from its reliance on tools like the Metasploit Framework, which may not detect all vulnerabilities,

particularly zero-day threats or those emerging post testing. Penetration testing is resource-intensive, requiring expertise, time, and computational power, making it less accessible for smaller organizations. Furthermore, testing often occurs in controlled environments, which may not fully replicate real-world attack scenarios, potentially leaving systems exposed to advanced hacking techniques. Ethical and legal constraints also limit testing on live systems, restricting its scope. Lastly, there is a risk of a false sense of security, as identifying some vulnerabilities may lead to overlooking others or underestimating evolving threats.

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]. 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.

[3]. 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.

[4]. 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.

[5]. Y. Kim, I. Kim, and N. Park, "Analysis of Cyber Attacks and Security Intelligence," in Mobile, Ubiquitous, and Intelligent Computing, vol. 274, J. J. Park, H. Adeli, N.Park, and I. Woungang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 489–494,2014

SYSTEM ANALYSIS

3.1 Existing System

The existing system surrounding Access Tools (RATs) on Android devices presents a dual reality of ethical applications and malicious exploitation. On one hand, RATs are widely misused by cybercriminals for activities such as data theft, extortion, and unauthorized device control. These malicious actors exploit vulnerabilities to steal sensitive information, blackmail users, or manipulate devices without consent. On the other hand, RATs have legitimate uses, including helping users recover

access to their devices after forgetting passwords or PINs and providing monitoring solutions for children, the elderly,Despite these benefits, the current system faces significant challenges. Sophisticated RATs often disguise themselves as legitimate applications, making detection difficult even for experienced users. Furthermore, a lack of user awareness about secure practices, such as avoiding unverified app sources, exacerbates the risks. To mitigate these threats, the Android ecosystem includes security measures such as antivirus tools, regular system updates, and app store vetting processes. However, issues like excessive surveillance in ethical use cases raise privacy concerns. Overall, while RATs offer valuable functionalities, their misuse poses a critical threat to Android device security, necessitating stronger preventive measures and greater user awareness.

3.1.1 LIMITATIONS :

INEFFECTIVE SECURITY :

- Existing antivirus and security applications may fail to detect advanced or disguised RATs.

LACK OF USER AWARENESS :

- Users often neglect basic security practices, such as avoiding unverified apps and keeping systems updated.

PRIVACY RISKS :

- Legitimate use of RATs, such as for monitoring, can lead to misuse or breaches of privacy.

APP STORE VULNERABILITIES :

- Malicious apps sometimes bypass app store security and vetting processes.

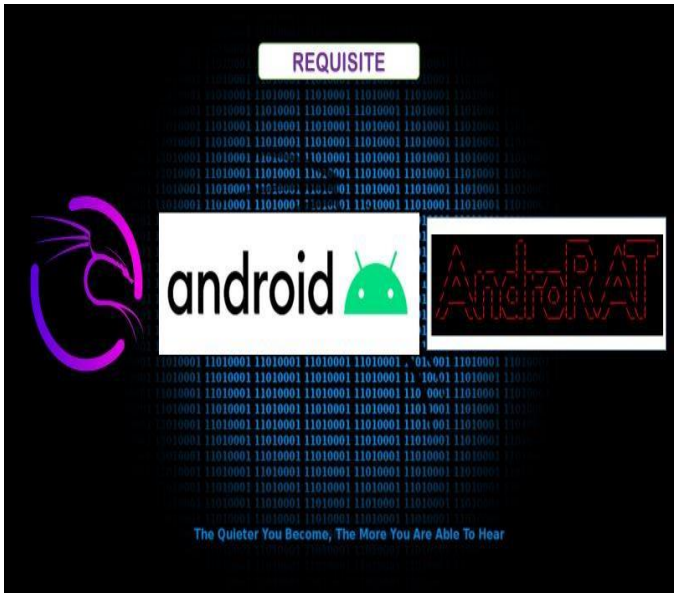
OVER-RELIANCE ON USER ACTION :

- Security depends heavily on users' vigilance, which is often inconsistent.

3.2 PROPOSED SYSTEM

3.2.1 Operating System Installation :

Kali Linux is a distribution specifically designed for penetration testing, including in android hacking. Kali Linux has several advantages in its use that make it easier for practitioners to do hacking. One of the advantages of Kali Linux is that it is equipped with a variety of complete hacking tools. Hence, users no longer need to install additional tools manually. Apart from that, Kali Linux also has an intuitive user interface so that users can efficiently operate the system and the tools provided. Another advantage is modifying and customizing the tools according to user needs through manual configuration or built-in features such as meta packages. Thus, Kali Linux is one of the right choices for android hacking practitioners in conducting security testing on the Android system.



3.2.2 Installation steps :

1. Download the Kali Linux ISO file from the official Kali Linux website.

2. Prepare an empty USB flash drive with a minimum capacity of 4 GB.

3. Download and install the Rufus application to create a bootable USB. Open the Rufus application and select the USB flash drive to use.

4. In the "Boot selection" section, click the "SELECT" button and select the Kali Linux ISO file downloaded in step 1.

5. Ensure the USB flash drive partition is in "MBR" mode, and the file system is "FAT32".

6. Click the "START" button and wait until the bootable USB creation process is complete.

7. After the process, insert the USB flash drive into the computer where Kali Linux will be installed.

8. Set the BIOS settings to boot from the USB flash drive the first time. The method depends on the type and brand of your computer or laptop.

9. Select the "Graphical Install" option on the Kali Linux boot menu after successfully booting from the USB flash drive.

10. Follow the on-screen installation instructions, including selecting the language, time zone, and hard drive partition to use.

11. Select the root password setting and create a new user account.

12. Wait for the installation process to finish. Once done, Kali Linux is ready to use.

3.2.3 Remote Administration Tool Installation :

1. First, ensure that Kali Linux is installed and updated with the latest version.

2. Then, open the terminal on Kali Linux and run the command "git clone https://github.com/AndroidRAT.git" to download the source code from GitHub.

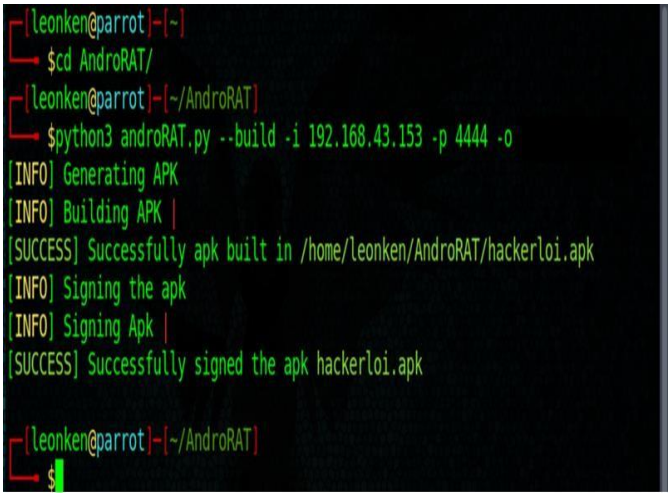
3. After successfully downloading, enter the RAT directory with the command "cd Android-RAT".

4. Next, run the command "sudo sh AndroRAT.sh" to start the installation process on Kali Linux.

5. Wait for the installation process to finish, and after that, open the tool by typing the command "sudo sh AndroRAT".

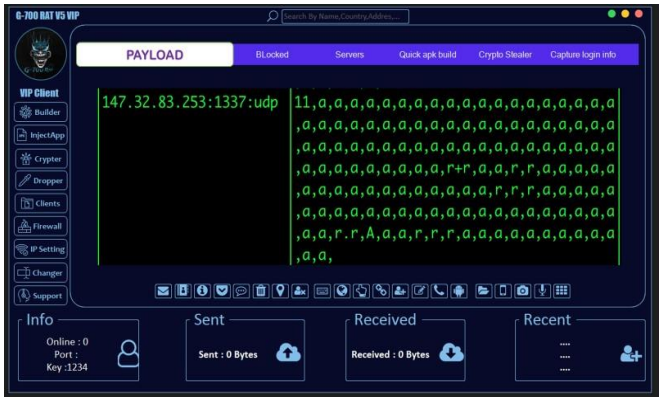
6. After the installation users can start creating an Android application that will be injected with the Remote Administration payload.

7. Once done, Remote Administration Tool is ready to hack the target Android device.



3.2.4 Social Engineering Techniques :

Social engineering methods of installing RAT applications can be carried out in various ways, such as creating fake messages or emails that look genuine, creating websites or pages that mimic the appearance of official sites, or using other tactics that trick the target into downloading and installing applications that contain malware. These techniques usually involve psychological manipulation of the target, such as making fraudulent offers or promises, intimidating or threatening, exploiting curiosity, and taking advantage of the target's trust or ignorance. It is important to remember that these actions are illegal and may harm others. Therefore, it is crucial for technology users always to be vigilant and careful when obtaining informationor downloading applications from unknown sources. In addition, it is also essential to update the device security system and use the latest security software to avoid harmful malware attacks



3.2.5 Methods of Data Collection and Prevention :

Collecting personal data using hacking RAT on Android devices can be done in various ways. One common way is sending malicious applications embedded with

RATs to the target device. Once the application is installed on the target device, RATs can collect personal data such as text messages, phone calls, and browsing history. In addition, RATs can also be used to take control of the target device, such as activating the camera or microphone and recording user activity without their knowledge. Another method is to use phishing techniques, such as sending fake messages or emails that trick users into providing their personal information or clicking on links containing malicious applications embedded in RATs. In addition

SYSTEM REQUIREMENTS

4.1. Hardware Requirements:

System : Intel i3 Processor (or equivalent)

Hard disk : 100Gb Minimum

Monitor : 15 Inch VGA Color

RAM : 4 GB

4.2. Software Requirements: Operating System : Windows 10 Platform : Kali Linux

Web Framework : AndroRat

Development Environment : Virtual Box

4.3 Software Description

Linux

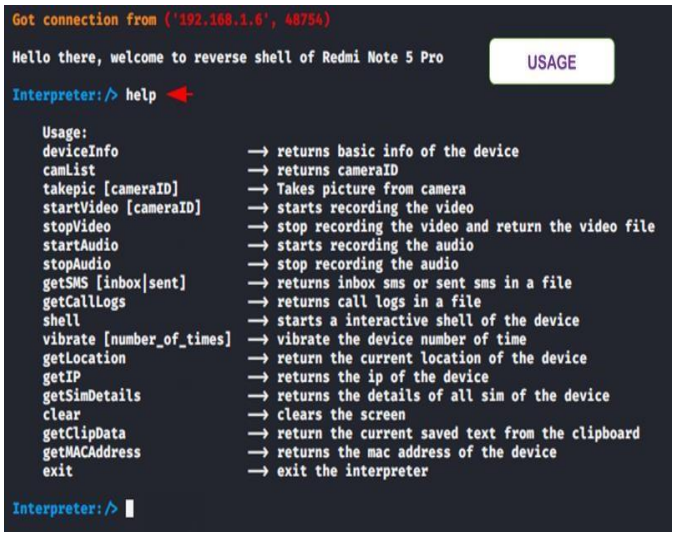
Linux is an open-source operating system known for its stability, security, and flexibility. Widely used in servers, development environments, and ethical hacking, it supports various distributions like Ubuntu, Fedora, and Kali Linux. Its command-line interface (CLI) and extensive tools make it a favorite among IT professionals and cybersecurity experts.

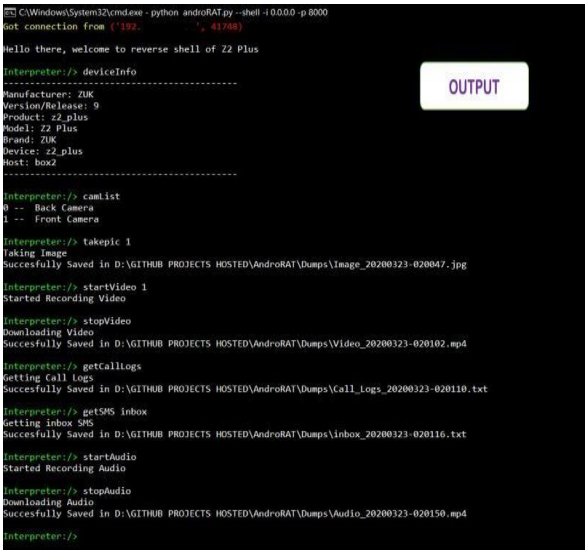
AndroRAT

AndroRAT (Android Remote Administration Tool) is a hacking tool designed to remotely control Android devices. Originally developed as a research project, it has been misused for malicious purposes like data theft and spying.

VirtualBox

VirtualBox is a free and open-source virtualization software that allows users to run multiple operating systems on a single machine. Its versatility makes it a valuable tool for software developers and cybersecurity professionals.





OUTCOME

The Expected outcome of this project to achieve several critical outcomes. First, it will identify vulnerabilities in Android devices' systems and networks that are susceptible to exploitation through social engineering methods. This includes demonstrating how attackers can deploy a Remote Administration Tool (RAT) to compromise user privacy and security. The research will provide insights into the mechanisms of data theft, such as accessing personal information, call logs, and remotely manipulating device features like cameras and microphones. Additionally, the study will highlight the effectiveness of using Kali Linux for Android security testing, showcasing its intuitive interface, customizable tools, and advanced features. Ultimately, the findings will contribute to raising awareness about social engineering risks and promoting better security practices among Android users.

5.1 Conclusion :

The use of social engineering techniques in installing Remote Administration Tools on Android devices is very effective. In this case, users convinced respondents to install applications containing Remote Administration Tools by making convincing fake messages or phone calls. In addition, the research results also show that security on the Android system is still very vulnerable to Remote Administration Tools attacks that can take over the device remotely and collect users' data without their knowledge. Therefore, it is necessary to take better precautions and safeguards on Android devices to prevent malicious Remote Administration Tools attacks.

Some steps to avoid these attacks include downloading apps only from trusted sources, keeping your Android device updated with the latest security patches, and installing reliable antivirus software.

REFERENCES

[1] A. R. Maulana and D. P. Wardhana, "Remote Administration Tool (RAT) Implementation using AhMyth and Social Engineering Techniques," 2020 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM), Surakarta, Indonesia, 2020, pp. 1-5, doi: 10.1109/CENIM51083.2020.9317252.

[2] W. R. Pratama and A. F. T. Riyadi, "Uji Penetrasi Remote Administration Tool pada Android dengan Teknik Social Engineering," Jurnal Teknologi Informasi dan Komunikasi, vol. 8, no. 2, pp. 56-62, 2022.

[3] R. H. Putra, M. N. Huda and T. A. Wisesa, "Android Hacking Using AhMyth RAT with Social Engineering Techniques," 2020 4th International Conference on Informatics and Computing (ICIC), Jakarta, Indonesia, 2020, pp. 1-5, doi: 10.1109/IAC50653.2020.9259369.

[4] S. Pradana, D. D. Setiawan and N. E. Darmawan, "Remote Administration Tool(RAT) Implementation using AhMyth RAT and Social Engineering Techniques," 2021 International Conference on Advanced Informatics: Concept, Theory and Application(ICAICTA),Malang,Indonesia,2021,1-6, doi: 10.1109/ICAICTA51487.2021.9488906.

[5] S. R. S. Maharjan, S. Maharjan and S. Adhikari, "Social Engineering Techniques and the Use of Remote Access Trojans (RATs) in Android Devices," 2019 4th International Conference on Computing, Communication and Security (ICCCS), Rome, Italy, 2019, pp. 1-6, doi: 10.1109/CCCS.2019.888718