Android Device Hacking : TheFatRat and Armitage

Ebin Thoppil
Amal Jyothi College of Engineering
Kanjirappally, India
ebinthoppil@mca.ajce.in

Snehamol Sibichan
Amal Jyothi College of Engineering
Kanjirappally, India
snehamolsibichan@mca.ajce.in

Vysakhi Viswanath
Amal Jyothi College of Engineering
Kanjirappally, India
vysakhiviswanath@mca.ajce.in

Rini Kurian
Amal Jyothi College of Engineeri
Kanjirappally, India
rinikurian@amaljyothi.ac.in

***Abstract*—Android is a fast-growing and popular operating system among Smartphones and portable devices.Cyber attacks are on the rise against Android devices due to misuse of android applications resulting in the invasion of the victim's privacy. One possible and appropriate way to avoid hacking of system and network penetration testing.**

Paper summarily describes penetration testing, Kali Linux tools such as Armitage and TheFatRat. These tools have proved to be effective in Android exploitation. By using TheFatRat, generate payload using msfvenom. It creates a backdoor to get access to the system, using the graphical user interface of Armitage, simply exploits the android device. Armitage is a Metasploit framework and finds any vulnerability on the target system then it will automatically hack that system.

Keywords—TheFatRat, Armitage, Meterpreter, MSF venom, Metasploit framework, Payload, Backdoor.

I. INTRODUCTION

Android devices are timely upgraded, replacing and adding tens of thousands of files on a live system in the presence of a large amount of user data and existing apps. The open nature of Android, a large number of malwares are hidden in android apps that threaten Android security. Penetration testing can be used to verify that new and existing applications that are not vulnerable to a security risk that could allow unauthorized access to resources. There are several freeware and commercial tools that perform specific functions. Penetration testers are using a vulnerability scanner to identify problems with the configuration of a system. After finding the vulnerability, a pentester's main goal is to Breach all types of security and take the remote access of the server. For doing this we use the Metasploit framework.

TheFatRat a massive exploitation tool. Easy tool to generate backdoor and post-exploitation attacks like browser attack, etc. This tool compiles a malware with payload and then the malware can be executed on windows, android, etc. Armitage is an interface of the Metasploit Framework that recommends exploits, visualizes targets, and also disclosure the post-exploitation features in the framework. Armitage is a graphical user interface.

TheFatRat and Armitage are combined to exploit an Android device. TheFatRat is used to create payload and Armitage is used to exploit the android device.

II. IMPLEMENTATION

A. PENETRATION TESTING

The penetration test is to verify that networks and systems are not vulnerable to a security risk that could allow unauthorized access to resources.

B. ANDROID EXPLOITATION

Exploitation is Nothing but finding the vulnerabilities. An exploit is a form of malicious code that takes advantage of a flaw or vulnerability in an operating system or piece of software with the intent to breach security to alter a user's settings without their knowledge.TheFatRat and Armitage are combined to exploit an Android device.

Computer experts have devised a new utility that can easily craft custom malware strains. The tool TheFatRat can compile the viruses with popular payloads and then compile the resulting file to run a specific platform. TheFatRat is a very easy tool for generating a backdoor or payload. You can create a full undetectable (FUD) payload by using this tool so antivirus cannot detect it as a virus.

The tool Armitage is used to run exploitation in a vulnerable device. Once Armitage finds any vulnerability on the target system then it will automatically hack that system. With the help of Graphical User Interface, it becomes so easy to hack any system. This tool performs different types of attacks if your system is vulnerable to any of these attacks. You can fix that vulnerability a virus.

TheFatRat
TheFatRat is a simple to use tool which helps in generating backdoors, system exploitation, post-exploitation attacks, browser attacks, DLL files, FUD payloads against Linux, Mac OS X, Windows, and Android. It can be combined with msfvenom which can be then utilized to utilize a reverse shell.

Armitage
Armitage is a graphical user interface of Metasploit framework that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework.

MSF VENOM
Msfvenom is a command-line instance of Metasploit that is used to generate and output all of the various types of shellcode that are available in Metasploit.

Metasploit
The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection.

Meterpreter
Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. Meterpreter is deployed using in-memory DLL injection.

Backdoor
A backdoor is a malware type that negates normal authentication procedures to access a system. Backdoor installation is achieved by taking advantage of vulnerable components in a web application. Once installed, detection is difficult as files tend to be highly obfuscated.

Payload
The payload can be considered to be somewhat similar to a virus. A payload is a set of malicious codes that carry crucial information that can be used to hack any device beyond limits that you can't imagine.

COMMON TERMS

Exploit

A piece of code written to take advantage of a particular vulnerability in the system.

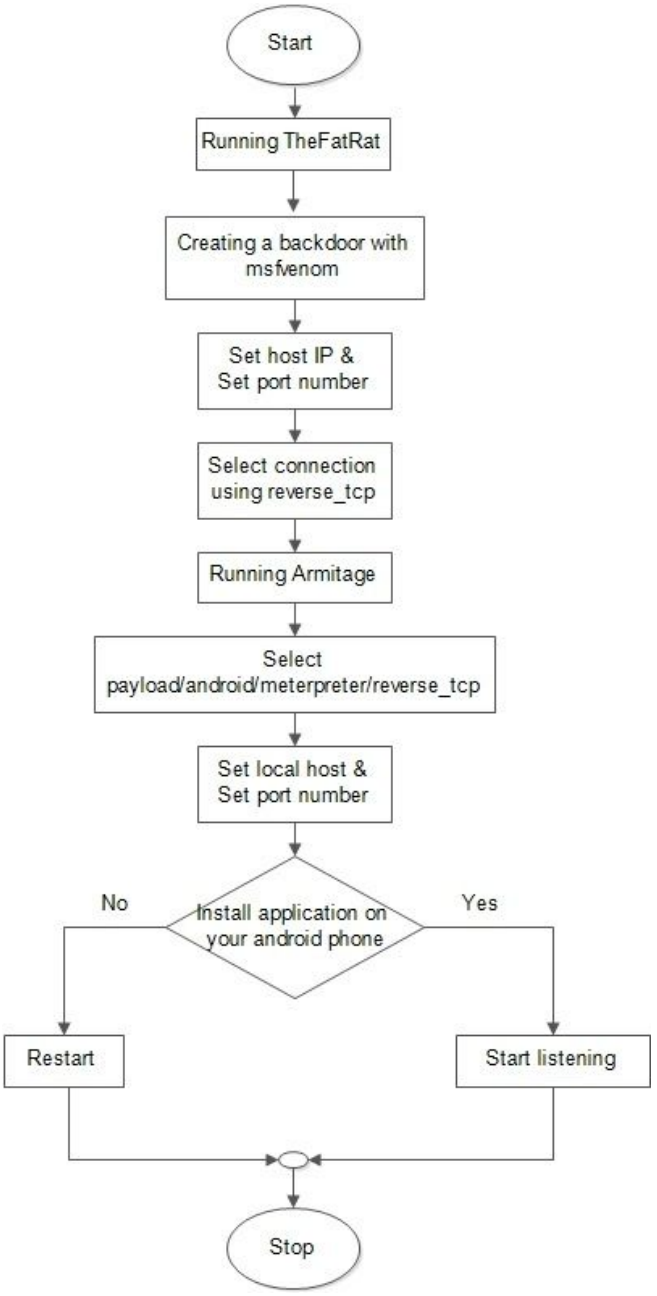
LHOST

IP address used by attacker to communicate with victim.

LPORT

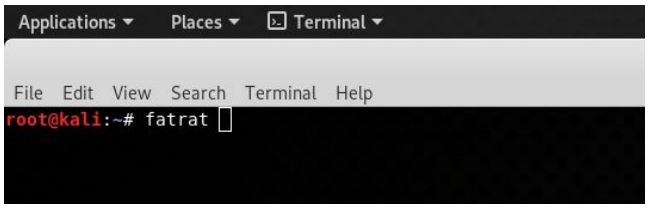
Port used by attackers to listen to victim devices.

C. STEPS TO PERFORM ETHICAL HACKING



STEP 1
Downloading and installation of TheFatRat
Downloading process is simply a git clone. The command used :
git clone https://github.com/Screetsec/TheFatRat.git

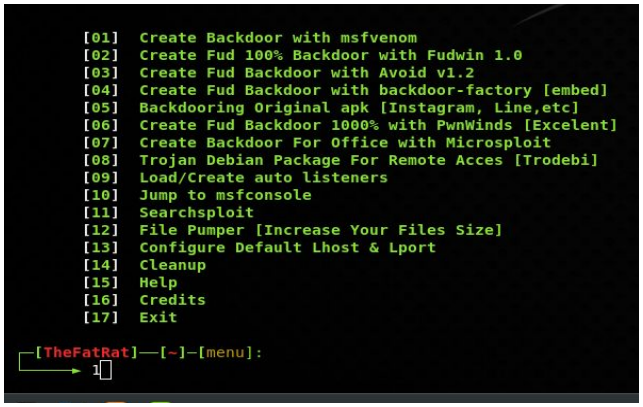
STEP 2
Run TheFatRat
#fatrat



STEP 3

Create a backdoor with msfvenom

To inject the payload into a victim's device first attacker needs to create a backdoor.



STEP 4

Select the payload

SIGNED ANDROID>> FatRat.apk

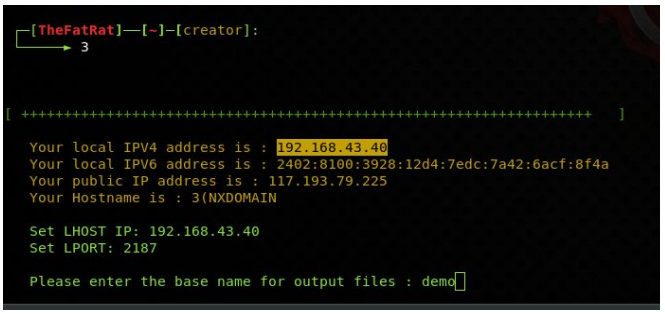
Set the Host IP address and Port number.

STEP 5

Enter a base name for the payload.

Select android/meterpreter/reverse_tcp

Payload is created and the attacker needs to inject the payload into the victim's device.



STEP 6

Install the apk payload on your Android phone

Install the payload in victims device by using any of the following methods.

- Data cable
- Pendrive
- Shared link through mail.

STEP 7

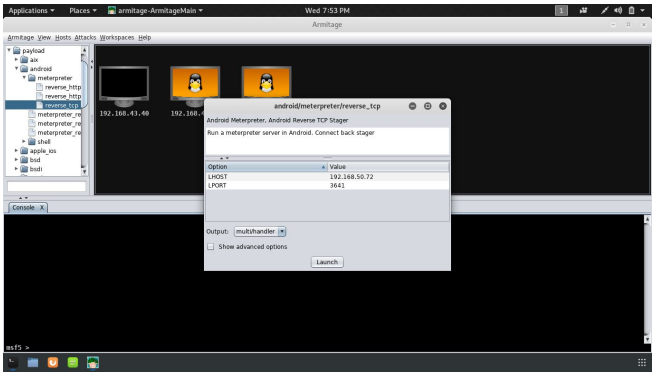
Start Armitage

#armitage

Victim successfully installed the apk payload and the attacker needs to set up a listener.

Select payload > android > meterpreter > reverse_tcp

The multi/handler window will appear, then the attacker needs to set the LPORT.

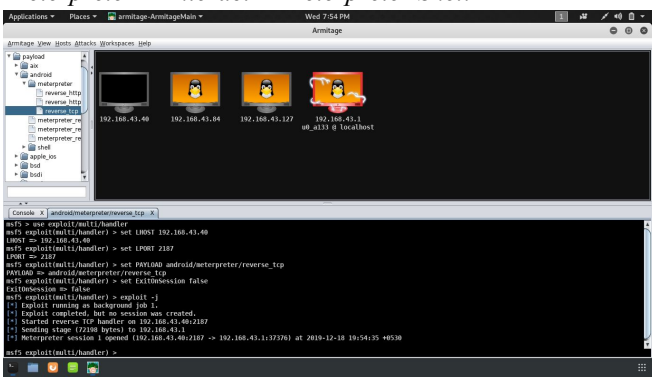


STEP 8

START LISTENING

Once the apk payload has been installed and opened in the victim's device, it will create a remote session with the attacker's machine. The target machine on Armitage should now turn red with a lightning effect. At this point the attacker can open a meterpreter prompt by right clicking on the host.Then select the meterpreter shell.

Meterpreter > Interact > Meterpreter Shell



STEP 9
ACCESSING FILES ON VICTIM DEVICE
meterpreter > Explore > Browse files
Attacker can download the files from the victim's device from here.

BASIC OPTIONS:

- **webcam_snap -** Take a snapshot.
- **webcam_stream-** Play a video stream.
- **webcam_list -** List the camera types in the device.
- **dump_calllog-** View the call details.
- **dump_sms –**To retrieve messages from the victim's phone.
- **set_audio_mode –**Set the android device in silent to ringing mode.
- **send_sms –**Send message from victims to another.
- **record_mic-**Record audio from victim's phone using mic
- **sysinfo-**Retrieve OS version of victim's phone

III. LITERATURE REVIEW

Himanshu Shewale, Sameer Patil, Vaibhav Deshmukh and Pragya Singh [1].Android platform allows developers to freely access and modify the source code. But at the same time it increases the security issue. A user is likely to download and install malicious applications written by software hackers.Android architecture: the Linux Kernel and lower levewethe l tools, System Libraries, the Android Runtime, the Application Framework and Application layer on top of all. Each layer provides different services to the layer just above it. This will analyze the existing threats and security weaknesses. The vulnerabilities found in android according to various layers of the android architecture from which they originated,Linux Kernel Layer, Libraries Layer, Application Framework Layer, Applications Layer and External Drivers.Android must timely introduce new security enforcement and exploit mitigation techniques. store. In the coming years, the users can trust enough to do even their banking transactions from smart phones.

Zheran F,Weili Han,Yingjiu Li [2]. Android security has been built upon a permission based mechanism which restricts accesses of third-party Android applications to critical resources on an Android device.numbers.Third-party application developers can leverage various smartphone sensors such as GPS, cameras, and microphones, then create applications that do more than what they claimed so as to collect users' private information stealthily

V. Santhi, Dr K. Raja Kumar, B. L. V. Vinay Kumar[3]. Penetration testing is a critical step for the development of any IT application under secure product or system. The IT sector today should be more aware of penetration testing. The computer security is the most important factor in the e-environment.Penetration Testing helps you to secure a computer system, network or web applications that allows you to gain high security issues which also helps to find vulnerabilities that an attacker could exploit. Penetration tools had a lot of attention as it doesn't have limitations in their production. Penetration testing tools that are specifically used in every distinct level of testing.

Umesh Timalsina,Kiran Gurung [4].The Metasploit framework is an open source tool for performing an exploit against a remote target machine.Penetration tester can use the tools provided by the framework to exploit the vulnerabilities present in the remote system.It offers more than one interface to its underlying functionality, including console, command line, and graphical interfaces.That are MSFconsole, MSFcli and Armitage respectively.

Yin Zhang ,Vern Paxson[5]. A backdoor is a mechanism introduced into a computer system to facilitate unauthorized access to the system.While backdoors can be installed for accessing a variety of services, of particular interest for network security are ones that provide interactive access.These are often installed by attackers who have compromised a system to ease their subsequent return to the system.

IV. PROS AND CONS

Pros:

• Open source

• Frequently updated

• Easy to deploy user specific exploit

Cons:

• Can crash your system if not used wisely.

• Requires deep knowledge for exploit development.

V. PREVENTION

The backdoor application when installed and turned on the mobile allows attacker to read, write and modify data. Cautions are.

- Never permanently enable installing of Apps from "Unknown sources ".
- Never take your phone to important meetings or anywhere you don't want people listening.
- Keep your Android up to date.
- Installing antivirus software on your Android device.

CONCLUSION

Improvising the security of an Android OS is very important to safeguard the user's privacy and confidential information. The Android operating system uses the permission-based model to access various resources and information. Android shared user ID is one of the major reasons for misusing app permissions. Like many security tools, the combined working of TheFatRat and Armitage provide a user friendly interface and easy to deploy user specific exploit. These tools allows penetration testers and security analysts to ensure everything is behaving properly using a combination of manual testing and automation to ensure full visibility.

References

[1] Himanshu Shewale, Sameer Patil, Vaibhav Deshmukh and Pragya Singh,"Analysis of Android vulnerabilities and modern exploitation techniques", ICTACT Journal on communication Technology,March 2014

[2] Zheran F,Weili Han,Yingjiu Li [2]."Permission based Android security: Issues and countermeasures"

[3] V. Santhi, Dr K. Raja Kumar, B. L. V. Vinay Kumar, "Penetration testing using Linux Tools: Attacks and Defense Strategies", International Journal of Engineering Research & Technology (IJERT).

[4] Umesh Timalsina, Kiran Gurung."Metasploit Framework in Kali Linux" ,Department of Electronics and Computer Engineering, IOE, Thapathali Campus, Thapathali, Kathmandu March 10, 2017

[5] Yin Zhang and Vern Paxson, "Detecting Backdoors"

[6] Tiwari Mohini, Srivastava Ashish Kumar and Gupta Nitesh had, "Review on Android and Smartphone Security", Research Journal of Computer and Information Technology Sciences.

[7] Himanshu Gupta, Rohit Kumar, "Protection against penetration attacks using Metasploit", 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)

[8] S.Angel,Dr.S.Sarala,"A study on Penetration Testing",International Journal of Advanced Research in Computer Science,Volume 2, No. 5, Sept-Oct 2011

[9] Aileen G. Bacudio,Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones,"An overview of penetration testing",International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[10] Devanshu Bhatt,"Modern Day Penetration Testing Distribution Open Source Platform - Kali Linux",International journal of scientific & technology research,volume 7,issue 4,April 2018.

[11] Seema Rani1, Ritu Nagpal,"Penetration Testing using metasploit framework:An ethical approach", International Research Journal of Engineering and Technology (IRJET),Volume: 06 Issue: 08 ,Aug 2019

[12] Pawan Kesharwani1, Sudhanshu Shekhar Pandey, Vishal Dixit, Lokendra Kumar Tiwari, "A study on Penetration Testing Using Metasploit Framework", International Research Journal of Engineering and Technology (IRJET)

[13] Huasong Meng, Vrizlynn L.L. Thing, Yao Cheng, Zhongmin Dai,Li Zhang, "A survey of Android exploits in the wild", Institute for Infocomm Research, Agency for Science, Technology and Research, Singapore, 138632, Singapore.

[14] Zhenlong Yuan, Yongqiang Lu, and Yibo Xue, "DroidDetector: Android Malware Characterization and Detection Using Deep Learning"

[15] Karthick S,Dr. Sumitra Binu, "Android Security Issues and Solutions",International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2017)

[16] Belal Amro, "Malware detection techniques for mobile devices",International Journal of Mobile Network Communications & Telematics (IJMNCT) Vol.7, No.4/5/6, December 2017

[17] P. D. Meshram,Dr. R.C. Thool, "A survey paper on vulnerabilities in Android OS and Security of Android Devices"

[18] Carlos Joshua Marquez, "An Analysis of the IDS Penetration Tool: Metasploit"

[19] Mario Linares-Vásquez, Gabriele Bavota, Camilo Escobar-Velásquez, "An Empirical Study on Android-related Vulnerabilities"

[20] Daoyuan Wu, Debin Gao, Eric K. T. Cheng, Yichen Cao, Jintao Jiang, Robert H. Deng, "Towards Understanding Android System Vulnerabilities:Techniques and Insights"

[21] Linxi Zhang, "Smartphone App Security: Vulnerabilities and Implementations".

[22] Huicong Loi, Aspen Olmsted, "Low-cost Detection of Backdoor Malware"

[23] Zarni Aung, Win Zaw, "Permission-Based Android Malware Detection"