International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5481
***Article Received**: 28 March 2021 **Revised**: 19 April 2021 **Accepted**: 30 April 2021 **Publication**: 31 May 2021*

Access Android Device Using The FatRat and Metasploit

Karan
Global Institue Of Technology
Jaipur, India
17egjcs856@gitjaipur.com

Palvinder Singh
Global Institute of Technology Jaipur,India
17egjcs107@gitjaipur.com

Amit Bohra
Assistant Professor
Global Institue Of Technology, Jaipur, India
bohraamit7@gmail.com

Abstract—At present, smartphones are widely used for both business and personal purposes. As we all know that android is the popular mobile operating system. Like Windows operating system vulnerability the android has also vulnerability. And on the basis of these vulnerabilities, an attacker can obtain a user's privacy data. But one possible way to avoid accessing of system and network i.e. penetration testing

This paper describes penetration testing, Kali Linux tools such as Metasploit and TheFatRat. These tools have proved to be effective in Android exploitation. For example, by using TheFatRat, create a payload using msfvenom. Furthermore, the Payload creates a backdoor to access the system, using Metasploit, which exploits the android device and finds the vulnerability and, according to vulnerability, access the victim's system.

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

I. INTRODUCTION

Nowadays, Mobile developers most commonly use Android OS to develop smartphones because of its performance, features, and services. Smartphones provide services such as phone calls, internet services, online and offline games, email, video calls, social networking apps, messaging, storing, and sharing files from one device to another. So, it is necessary to ensure security and safety in android devices. With the open nature of Android, a large number of malware are hidden in android apps that threaten Android security. Penetration testers use the vulnerability scanners, and through this scanner, they identified the vulnerability in a system. After getting the vulnerabilities, penetrations testers take the server's remote access to breach the all types of security by using the Metasploit framework.

TheFatRat tools is a free and open-source tool. Through this tool, we generate a backdoor. FatRat convened a malware with Payload, and then the malware can be executed on Windows, Android, etc.

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

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5481
***Article Received**: 28 March 2021 **Revised**: 19 April 2021 **Accepted**: 30 April 2021 **Publication**: 31 May 2021*

II. IMPLEMENTATION

I. PENETRATION TESTING

Penetration testing is a protective and unauthorized effect of accessing the computer system to find the vulnerabilities from various viewpoints.

II. ANDROID EXPLOITATION

With the help of exploitation, we find the vulnerability. Here exploitation is a malicious code and breaches the security of a system without user knowledge. TheFatRat and Metasploit are combined to exploit an Android device. The tool TheFatRat can compile the viruses with payloads and compile the resulting file to run a specific platform. Through TheFatRat, we generate a backdoor or Payload. It means you can create a full undetectable (FUD) payload using this tool, which means antivirus cannot detect it as a virus. The Metasploit Framework is used to run exploitation in a vulnerable device. Once Metasploit finds any vulnerability on the target system, then it will automatically access that system. If you are using this tool and your system is vulnerable, you can perform any other type of attack through this tool. For example, you can fix the vulnerability of a virus.

TheFatRat

TheFatRat is a simple to use tool which helps in generating backdoors, system exploitation, post-exploitation attacks, browser attacks, Windows, and Android. The combination of MSF payload and Msfencode make a single framework that is TheFatRat.

MSF VENOM

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

Metasploit

The Metasploit framework is a potent tool for attackers to customize this tool according to their operating system. Metasploit is a Perl-based portable network tool and in 2007 is written in Ruby language. And it provides a platform, through this, you can access the device remotely and maintain the access, detect, IPS, IDS, etc.

Meterpreter

It is a Metasploit attack payload, and the Payload provides a shell. Through this shell, an attacker can explore the victim's machine and execute the code

Backdoor

A backdoor is a method, and with the help of a backdoor, a penetration tester or an attacker can enter into the victim's machine.

Payload

The Payload is considered similar to a virus. A payload is a set of malicious codes that ship sensitive information, and through this, we can access any device and take advantage.

COMMON TERMS

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

LHOST
An attacker uses the IP address of localhost to communicate with the target machine.

LPORT

The Port of localhost, which attackers use to listen to the target machine.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5481
Article Received: 28 March 2021 Revised: 19 April 2021 Accepted: 30 April 2021 Publication: 31 May 2021

III. STEPS TO PERFORM ACCESS ANDROID DEVICES

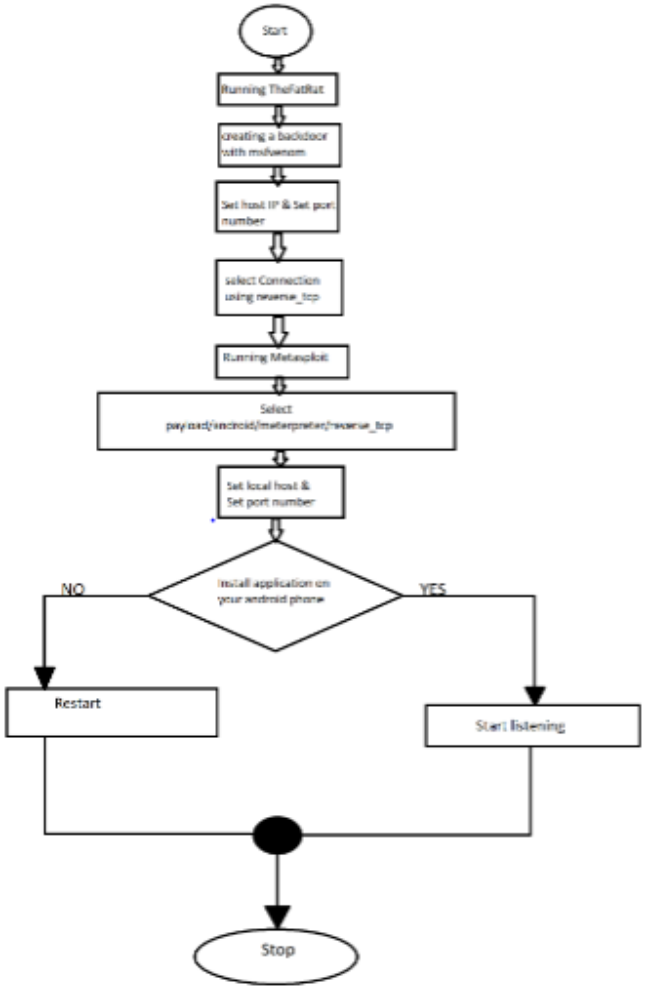

Fig 1. Steps to Accessing the Devices.

STEP 1

Downloading and installation of TheFatRat

First of all, download theFatRat from GitHub gitclonehttps://github.com/Screetsec/TheFatRat.git

STEP 2

After that, run TheFatRat

#Fatrat

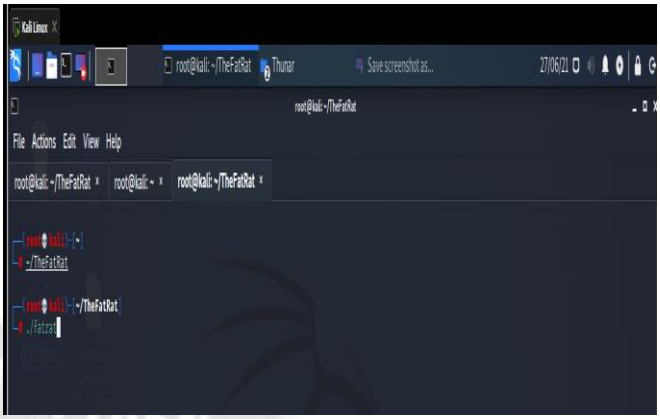

Fig 2. Run the FatRat

STEP 3

Now create a backdoor with msfvenom

First of all, an attacker needs to create a backdoor because an attacker injects a payload into the target machine through the backdoor.

Fig 3. Create backdoor with msfvenom

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5481
***Article Received**: 28 March 2021 **Revised**: 19 April 2021 **Accepted**: 30 April 2021 **Publication**: 31 May 2021*

STEP 4

Choose the Payload

SIGNED ANDROID>> FatRat. apk
In this step, set the LHOST IP address and Port number.

Fig 4.choose the payload

STEP 5

Enter a base name for the Payload.

Select android/meterpreter/reverse_tcp
When the Payload is created, then the attacker needs to inject it into the target machine. And the base name for the file, i.e., game. apk

Fig 5. Set the name of apk

STEP 6

Then install the apk payload on your Android phone

Install the Payload in the target machine by using any of the following methods.

- Data cable
- Pen drive
- Shared link through the mail.

STEP 7

Start Metasploit

#Msfconsole
Then we use *exploit/multi/handler*
Select payload > android > meterpreter > reverse_tcp
The multi/handler window will show, then the attacker needs to set the LHOST & LPORT.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5481
***Article Received**: 28 March 2021 **Revised**: 19 April 2021 **Accepted**: 30 April 2021 **Publication**: 31 May 2021*

Fig 6. Set the LHOST & LPORT in Metasploit

STEP 8

Start Listening

Once the apk payload has been installed and opened in the target machine, it will create a remote session with the attacker's device. Then after that, an attacker can access some confidential information like call logs, SMS, sysinfo, etc.

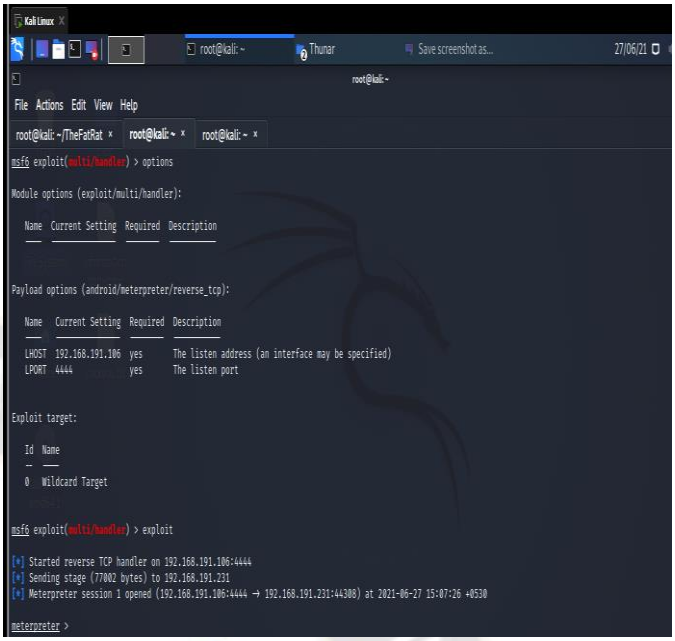

Fig 7. Opening of Metasploit Session

STEP 9

Accessing files on victim on victim device

meterpreter > Explore > Browse files
An attacker can download the files from the victim's device.

BASIC OPTIONS:

- **webcam_snap -** Take a snapshot.
- **webcam_stream-** To 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 from silent to ringing mode.
- **send_sms –** Send messages from one victim to another.
- **record_mic-** Record audio from victim's phone using mic
- **sysinfo-** Retrieve OS version of victim's phone.

STEP 10

Secure Android Devices using Malwarebytes Security

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5481
***Article Received**: 28 March 2021 **Revised**: 19 April 2021 **Accepted**: 30 April 2021 **Publication**: 31 May 2021*

In this step the users can secure their devices through Malwarebytes Security from malicious application.

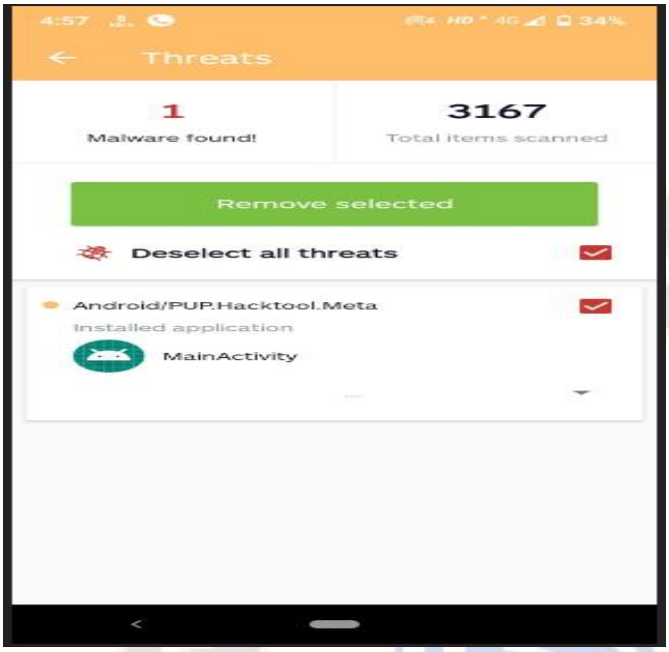

Fig 8. Malwarebytes security tools

III. LITERATURE REVIEW

A. E Thoppil, S Sibichan, V Viswanath, R Kurian. Android Security uses the technique of permission-based mechanism to restrict or access the various resources. Nowadays, security plays an essential role in android phones because you can see the mobile phone in everybody's hands. Through security, we can save our user's privacy and sensitive information. Furthermore, it provides many tools like TheFatRat and Metasploit. Moreover, these tools allow penetration testers and security analysts to secure everything.

B. R Sajeev, S Joseph, S Biju, M Manoj. They say that android devices are used many functionalities, and these functionalities consist of many third-party applications. Furthermore, these applications can create a vulnerability for attackers. After that, the attacker can quickly get access to deployment, and we need to identify the vulnerabilities and secure all of these vulnerabilities by penetration testing tools.

C. Ajish V Nair Anusha Siby Aleena Mathew Mr. Ajith G S. They summarized that the Android device is unprotected after using the Metasploit framework and quickly retrieves android devices and steals confidential data the commands like webcam and dump_calllog. Moreover, the information's gain like it takes pictures, contacts and other information's. Furthermore, said that with the help of the Linux kernel layer, an attacker quickly gets access and steals the data.

D. Khulood Al Zaabi. He identifies the vulnerabilities in android devices and their connected third-party application. Furthermore, the application such as WhatsApp and GPS advises all GPS users and WhatsApp to be wary while using the android devices. Furthermore, it alerts all users and says that they learn the social engineering tricks and prevent themself from attackers. Moreover, he conducts a Stagefright code against vulnerable android devices by Text or MMS to trick the investigating and other exploitation vulnerabilities with android devices.

E. Maurice Dawson, Jorja Wright, Marwan Omar. They all suggest an antivirus application in smartphones for private information. Because in the computer we see many security functions like firewalls, antivirus, and cryptography but in android phones, these applications are not present in the market. So, as we compare the android devices with windows computers, the android devices are vulnerable. It is much easier to get access as compare to windows computers. Nowadays, smart users use Gmail, social media sites such as telegram, Twitter, Facebook, and other online purchasing site such as Flipkart, Amazon, Myntra, etc. It means the all the work are done by online services and sites in android phone. So, to security purposes, the attackers quickly get all of this information from your devices by accessing it.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5481
***Article Received**: 28 March 2021 **Revised**: 19 April 2021 **Accepted**: 30 April 2021 **Publication**: 31 May 2021*

IV. ADVANTAGES & DISADVANTAGES

ADVANTAGES

- It allows users to access source code.
- With the help of FatRat and Metasploit, we can find and arrange the security threats.
- With the help of FatRat and Metasploit, we can find loopholes or vulnerabilities in a device.
- With the help of these tools, we injected an apk file in 2 or 3 minutes.
- As we talk about cybercrimes, these tools are a high level of scope.

DISADVANTAGES

- In Metasploit, whenever the session is created after, it does not show the warning of a closed session**.**
- Security analysts or attackers may use the penetration testing tools like FatRat and Metasploit to collect confidential information about an organization's system or network.
- The Metasploit framework supports only a command-line interface in android devices.
- To exploit the android devices requires deep knowledge.

V. CONCLUSION

According to our research, we identified that the android devices and their connected third-party application are vulnerable. By which the attacker can then easily access the android devices and gets confidential information or important data. For example, using this information, he can take your pictures through the webcam command and also record the real-time data. So, all users should be very careful about using their smartphones and the developers need to identify the loopholes and vulnerability and ensure security to protect smartphones from the malicious application, by using some penetration testing tools.

In this research paper, we discussed how to access the android device as well as how to make secure the android device. Because when the penetration testers will access the android device then they can find out the vulnerabilities and loopholes in android devices and then they can secure the android devices using some penetration testing tools. In this paper, we also discussed the countermeasures of android devices because through these countermeasures the people will know about android security.

VI. COUNTERMEASOURES

Various countermeasures help to protect the android devices platform.

- Do not download too many application
- Avoid the auto-upload option of photos to cloud networks.
- Install the application from trusted sources such as the play store.
- Do not share the information when the GPS is enabling.
- Always configure a strong password with maximum length include digit, alphabet, special character.
- Set a timeout to automatically lock the phone when the users are not in use.
- Always remember that the minimum password length is eight characters.
- Remember to update the application from time to time.
- Use security tools to secure, detect, manage android devices.
- Use filter email- forwarding barriers.
- On the android device allows only signed applications.
- Download and Install the antivirus on Android devices.
- Never download the applications from unknown sources.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 9 Issue: 5
DOI: https://doi.org/10.17762/ijritcc.v9i5.5481
Article Received: 28 March 2021 Revised: 19 April 2021 Accepted: 30 April 2021 Publication: 31 May 2021

VII. REFERENCES

1. Thoppil, E., Sibichan, S., Viswanath, V., & Kurian, R. Android Device Hacking: TheFatRat and Armitage.
2. Sajeev, R., Joseph, S., Biju, S., & Manoj, M. A Collaborative Approach for Android Hacking by Integrating Evil-Droid, Ngrok, Armitage and its Countermeasures.
3. Siby, A., & GS, M. A. Android Hacking Using Msfvenom: Integrating NGROK.
4. Al Zaabi, K. (2016, June). Android device hacking tricks and countermeasures. In 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF) (pp. 1-10). IEEE.
5. Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smart phones. Journal of Information Systems Technology and Planning, 5(14), 40-60.