

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to use android phone to control meterpreter sessions](#)

Toast - May 11, 2018, 7:47 am

Hello everyone!

In this tutorial i'll teach you how to use your android phone to connect to your machine and control meterpreter sessions while you're away.

So let's begin!

Setting up the machine:

Let's begin with setting up your computer for this. For this tutorial i'll show you the steps for a linux machine.

You need to have an ssh server. Kali linux already has one installed, so we don't need to install one. If your kali machine does not have it installed then you can run the command:

"apt-get install openssh-server".

Now we need to start the ssh service. To do this open your terminal and type: "service ssh start". Now your computer's ssh server is active. To be able to access your machine through ssh however, you need to port forward your ssh server port. By default the port is 22.

Now for the final part of the machine setup, you have to create a new user. When you connect via ssh you will connect as this user.

To do this go in the upper right corner of your screen and click that little arrow, then select your current user username and go to account settings. After you do this a window with the title "users" will open. In the upper right corner of that window there is a button called "Add User...". Click it. Now another window opened. Here you will create the account. Make sure the account type is administrator. Now you just fill in the rest of the fields. In the password section select "Set password now" and set your password. When you are ready click the "Add" button in the top right corner of the window.

We are done with configuring the machine!

Now for the phone:

First you'll have to install "Termux" on your android phone. You can find it in the app store.

After you install it open it up and you're going to be greeted with a CLI.

You will use same commands as in linux for this.

Now we need to install openssh so you can connect to your machine. Type "pkg install openssh" and wait for it to install. When it is done you are ready to connect to your machine.

To connect we will use the account we set up earlier. Now type "ssh username@ip". Replace username with the username of the account and ip with your machine's ip.

After this you will be asked to enter the account's password. And now you are connected to your machine.

From now everything is as if you were in front of your computer. Set up a listener and whenever someone opens your metasploit payload you will be able to control everything.

Pro tip: set up a dns server using No-ip so you don't have to remember your IP.