

Forum:[Hack Forums](#)

Thread: [Hacking using a wifi pineapple \(or laptop\) - Part One - SSH](#)

FractumSeraph - December 24, 2015, 11:10 pm

I have made a small series of tutorials, intended for users of the WiFi Pineapple from Hak5. However, I have designed them in a way that they will also work on Kali Linux.

At the time of this writing, the new developer version of the NANO has been released, and there are a lot of questions about how to use the Pineapple without modules. To do this, I'm going to show you how to use SSH in order to control the pineapple.

Requirements: Network connection to pineapple (Ethernet, USB, or WiFi)[/*]

Complete the initial setup.[/*]

Kali Linux (Can be done on Windows, Mac, and Android as well using different apps, not sure about iOS)[/*]

Let's begin!

The first thing we need to do is connect to our pineapple. In order to do this, we need to know it's IP address. If you are connected directly to the Pineapple by Ethernet (Or USB on the NANO), then the default IP address will be 172.16.42.1.

Now that we know the address, we need some way of communicating with it. We will be using SSH.

What is SSH? (In my non-technical terms) -> Spoiler [\(Click to View\)](#)

If you're familiar with windows, you've probably heard of Command Prompt, the black window you type commands into, like ipconfig.

Linux has its own version of this, and when we are using SSH we are basically using the Linux command prompt remotely. If I were to leave my Linux computer at home while I went on vacation, I could connect to it with SSH and run commands as if I were at home.

Next, we need to open up Terminal.

On the default install of Kali, you will find this on the favorites bar on the right. Otherwise, you can go to Applications->Usual Applications->Utilities->Terminal

Once you click on the icon, a black box will open, similar to the command prompt in windows. To start an SSH session with the pineapple, we need to enter the following command

Code `ssh root@172.16.42.1` Then it will ask you for the root password of your Pineapple. (The one you made in the initial setup)

If this is your first time, it will likely ask you to verify a fingerprint just type 'y'.

Let me break this down a bit.

`ssh root@172.16.42.1`

'ssh' tell terminal what program you are wanting to use.

'root' is the user you are going to log in to.

'172.16.42.1' is the IP address you are connecting to. (Your Pineapple in this case)

Once you have done that, you will still be in a black box. This time however, the text on the top left will be root@pineapple, and on the MK5 The word WiFi Pineapple will be displayed in large letters. (I'm not sure on the NANO)

Now we are connected to the Pineapple. Any commands we type on this page are actually happening on the pineapple.

"Okay, but now what?"

Well now we need to learn about some general linux command line. If you find this boring, feel free to skip to my next tutorial which is going to show you how to do the stuff you'll actually be interested in. If you can manage however, continue reading and it will be better for you in the long run. It's not directly related to the pineapple, but it's good general knowledge of the linux command line.

Now that we are connected to our pineapple, lets just run a few commands to get used to it.

First let's run

Code ifconfigThis command is a lot like the 'ipconfig' command in Windows. It will show you all of the network devices attached to your pineapple, and some information on them. I haven't ordered mine yet, so I'll be using my laptop. Yours won't look exactly like mine, but it will be close.

There are three main connections you will be looking for.

Eth0 is your Ethernet connection. (USB on the NANO)

Wlan0 is your first wifi adapter

Wlan1 is your second wifi adapter

Again, just for practice, lets try turning one of them off, then checking again:

Code ifconfig wlan1 downCode ifconfig

Again, let's break this command down a bit.

ifconfig wlan1 down

ifconfig is the name of the program we are using.

wlan1 tell it which device we are choosing.

down tells it what we want to do to that device.

To turn the wifi card back on, all we have to do is run:

Code ifconfig wlan1 upNow that we are down with that we can just run

Code clearTo clear the page and get rid of all the clutter.

Next we are going to look at some basic directory traversal.

The first thing you need to do is to get your bearings. to do this, simply run the command

Code lsWhich will list all of the directories(folders) and files where you are.

Again, mine will be different than yours.

One thing to notice is that all of the directories(folders) are blue, and all of the files are white.

In order to move around, we will be using 'cd' which stands for Change Directory. As I said before, yours is different. I will be going into the Imms folder. Your device probably won't have this folder, so just choose the first one you see.

To open the Imms folder and check what's inside, I will be running
Code cd Imms
Code ls Just Change Imms to the name of whichever folder you choose.

As you probably know by now:

```
cd Imms  
ls
```

cd is the name of the program we are using.
Imms tell it what folder we are doing it on
ls shows what's inside the folder we are in.

In case we ever forget which folder that is, you will notice that it has been added (in blue) to the left of where we are typing.

Next, go back up a directory (Back to the place we were before), we use
Code cd ..(There is no space in between the periods, it just appears that way on some screens.)

Now, if we run ls again, we will see that we are back where we were before.

I will be ending part one here. In part two, I will show you how to sniff wifi packets, and do cool stuff.

In order to exit the SSH session you run:
Code exit Honestly I just click the X button myself, but technically this is the correct way.

In case these pictures get removed from Gyazo, I have also uploaded them here:
<http://www.mediafire.com/download/bfqub6t4kvuy4ao/SSH.zip>

I recommend you learn more about command line while you wait for my next post :p

http://linuxcommand.org/learning_the_shell.php

<http://lifehacker.com/5633909/who-needs-a-mouse-learn-to-use-the-command-line-for-almost-anything>

<https://www.linux.com/learn/tutorials/819973-how-to-use-the-linux-command-line-basics-of-cli>

[Part Two](#)

Sta.ze - December 24, 2015, 11:46 pm

Nice tutorial mate. Hope this helps users!

Pyrocynical - December 25, 2015, 8:18 am

Did you really have to make 3 threads?

Couldn't you comment the rest?

Anyways, good tut.

tjtheplanmaker - December 25, 2015, 9:40 am

(Dec 25, 2015 09:18 AM)SomeRandom Wrote: [\[CITE\]](#) Did you really have to make 3 threads?

Couldn't you comment the rest?

Anyways, good tut.

Get over it. Anyways, I've really been contemplating buying a wifi pineapple and this really really makes me want one. Is it really worth it?

FractumSeraph - December 25, 2015, 11:49 am

(Dec 25, 2015 10:40 AM)tjtheplanmaker Wrote: [\[CITE\]](#) Get over it. Anyways, I've really been contemplating buying a wifi pineapple and this really really makes me want one. Is it really worth it? That really depends. What do you plan on using it for?

Nearly everything you can do on the pineapple you can do with a laptop and a WiFi adapter. I just prefer the pineapple because I can carry it in my back pocket