

Forum:[Hack Forums](#)

Thread: [Use Kali Linux or a Raspberry Pi to clone Wifi and get data](#)

Chrissch2002 - August 23, 2017, 10:50 am

Is there a way to use Kali Linux (preferably a RPi) to clone or to run a wifi connection through and when devices connect monitor all their data which is sent through?

newgonhowzter - August 26, 2017, 4:24 pm

There are some builds for the raspberry pi that offer somewhat automated form of this. You can Google WarPi/war pi I think and it is meant for passive recon.

What you are attempting to do is quite a complex task and there are a few ways to go about this. You may want to look in to transparent squid proxy's, or alternatively you can set up you RPI as a firewall/router/DNS server (forward DNS requests to your server and this will allow you to redirect to a spoofed page if you are wanting to collect passwords etc)as it will get all the DNS requests to essentially see what is occurring on the network.

If you are setting up an RPI with Kali keep a few things in mind. The initial image I think sets the Hard drive partition to 8GB, so ensure you resize it correctly or it will get full fast as you are going to want to do an apt-get install Kali-Linux-Full or all or space to keep Pcap files etc. There is no "simple" way to set this up, if you want you can purchase something like the "Lan Turtle" which essentially gives you access to a reverse shell on whatever physical Ethernet connection it is attached too. You could also accomplish this by modifying a routers firmware but you would require SSH or Telnet access and the ability to add packages via flashing the routers firmware (check out merlin or tomato as they allow package management).

First establish what you want to do, then determine how you want to do it as it will depend on what your strong suit is. Capturing all traffic on a network (with the ability to see anything utilizing HTTPS is incredibly difficult as you need to bypass the certificate). You can also try using a server to manage your network or try something like spice network etc, check sourceforge as there are a ton of options. Depending on the level of access you have to the devices on the network. (physical or remote).

Molino. - August 27, 2017, 3:45 pm

If I understand correctly, you want to clone an existing wireless AP (access point), so people connect to yours instead of the already existing one, and so be able to monitor incoming data, sent from the users, right?

If that is the case, you are trying to create an Evil Twin AP, and there are two rather simple options (one easier then the other).

First step is to create an AP, and for this you have 2 options:

Method 1 (Manual AP)

First we'll have to manually create an AP using hostapd & dnsmasq (gives you much more control over the AP you create), which requires you to setup up the AP (will have to give it the same name of the one trying to clone), and routing the incoming data to the internet (so the AP still provides internet to a user). It will also require you to change the MAC address of your PI to the MAC address of the AP you are cloning (also simple).

Create AP: <https://www.raspberrypi.org/documentation/configuration/wireless/access-point.md>

Change Mac Address:

<https://linuxconfig.org/how-to-change-mac-address-using-macchanger-on-kali-linux>

Method 2 (Aircrack-ng)

This is a much more simple way to clone an AP. There are many tutorials on how to do this, but I'll drop some links on this method too (<https://www.aircrack-ng.org/doku.php?id=airbase-ng>). This method is much easier because it basically does everything from the last step, but with one or two commands, but you'll need a wifi card capable of packet injection.

After you create it, you'll now use aireplay-ng to de-auth everyone from the AP you're cloning, so people will disconnect from it, and connect back to yours (<https://www.aircrack-ng.org/doku.php?id=aireplay-ng>).

After this, you can use MITMf (<https://github.com/byt3bl33d3r/MITMf.git> or <https://github.com/CiuffysHub/MITMf>) to do a Man In The Middle Attack, which will allow you to capture any data sent by users, but currently this might not work for a simple reason. Even though MITMf does have a plugin to bypass HTTPS, some browsers like Chrome can prevent this bypass, meaning that you won't be able to see data from HTTPS connections (browser might even block the connection).

You can also try to use MITMf with beEF. This will allow you to use MITMf to inject the beEF hook into someone's browser, and thus allowing you to capture their cookies, and login to their sessions. But then again, some browsers have the capability to prevent these attacks.

All this can be used with Kali Linux installed on a Raspberry Pi, and everything is pretty straightforward.

I will post any missing links for tutorials when I get home.

If you need any help, feel free to ask, as I've done both multiple times.

kevy42 - August 28, 2017, 12:56 am

Dont forget to deauth the existing AP, to make ppl think its broke and connect to the other AP(urs)

Molino. - August 28, 2017, 6:30 am

(Aug 28, 2017 12:56 AM)WeedmasterOG Wrote: [\[CITE\]](#) Dont forget to deauth the existing AP, to make ppl think its broke and connect to the other AP(urs)

If you set your clone AP name and MAC address equal to the AP you're attacking, when you de-auth the users, they will automatically connect back to yours most of the time (had some times where it didnt work).

kevy42 - August 28, 2017, 7:05 am

(Aug 28, 2017 06:30 AM)Molino. Wrote: [\[CITE\]](#) If you set your clone AP name and MAC address equal to the AP you're attacking, when you de-auth the users, they will automatically connect back to yours most of the time (had some times where it didnt work).

damn thats conveeneant

SchwererGustav - August 28, 2017, 11:08 am

if you want to clone an AP just buy another wireless card which works on usb port ,and download pumpkinAP from github and you will be ready for it ,and i mean there is no need for the RPi for cloning the AP

Nomad.Null - August 29, 2017, 8:36 pm

Sure...take a look into Fruity-WiFi...basically the equivalent of the wifi pineapple for the raspberry pi. All you need is an extra Wireless-N card and a power bank. ?

lwristis - August 30, 2017, 4:42 pm

What wireless card do you recommend? I was looking for my company to purchase one