Cybergibbons

Reverse engineer, hardware hacker, security analyst, lock picker, heist planner. Definitely not involved in the Hatton Garden job.

Search …

Quick and easy fake WiFi access point in Kali

POSTED ON FEBRUARY 4, 2015 BY CYBERGIBBONS

I'm working on a project at the moment that requires me to observe traffic from an iOS/Android app to various external IPs.

The easiest way to do this is to setup a fake WiFi access point and use Wireshark to sniff the traffic. This is very easy in Kali Linux.

1. Connect the Kali box to the Internet

On my machine, this is as simple as connecting to my WiFi network "DoingAJob5G" using the built-in wireless card on my x220. I use the GUI provided with Kali.

Using *ifconfig* I can see that this adapter is called *wlan0*.

You could use wired Ethernet, then in all likelihood this will be *eth0* instead.

2. Connect an external WiFi adapter that is supported by hostapd

Categories

I'm using a USB TP-LINK TL-WN722N which is using an Atheros AR9271 chipset. These are cheap (£8-£10), powerful and reliable.

I suspect many USB WiFi adapters are compatible with *hostapd*, unfortunately I can't see a clear source documenting which ones.

Check it works by connecting to any network using Kali's GUI. This will save you hassle later if there are any driver or hardware issues.

3. Bring up the new wireless interface.

Use *ifconfig -a* to see the new wireless interface name:

```
wlan3     Link encap:Ethernet  HWaddr c0:4a:00:1e:64
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Bring this up as the gateway for your new wireless network. I am using 10.0.0.1/24 simply to avoid any chance of confusion with my internal NATed 192.168.0.1/24 network.

```
root@kali:~# ifconfig wlan3 10.0.0.1/24 up
root@kali:~# ifconfig wlan3
wlan3     Link encap:Ethernet  HWaddr c0:4a:00:1e:64
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
          TX packets:0 errors:0 dropped:0 overruns:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

4. Configure and run DHCP and DNS services

DHCP assigns IP addresses when clients connect, and DNS provides resolution of names to IPs.

Most wireless clients expect DHCP by default, so it is convenient to run a DHCP server. You can manually

set IP addresses, but it's really easier to do DHCP.

Running our own DNS server means that we can easily intercept and alter DNS queries, which can assist in setting up *man-in-the-middle* attacks.

A piece of software called *dnsmasq* does both DHCP and DNS and is very simple to setup.

First, install *dnsmasq*:

```
1 apt-get install dnsmasq
```

Next, create a config file *dnsmasq.conf* as follows:

```
1 interface=wlan3
2 dhcp-range=10.0.0.10,10.0.0.250,12h
3 dhcp-option=3,10.0.0.1
4 dhcp-option=6,10.0.0.1
5 server=8.8.8.8
6 log-queries
7 log-dhcp
```

This is about as simple as it gets. Only listen on *wlan3*, our additional wireless adapter. Hand out DHCP addresses from 1*0.0.0.10-10.0.0.250*. DHCP option 3 is the gateway, DHCP option 6 is the DNS server – both of these should be set to our *wlan3* IP of *10.0.0.1*. *server* specifies upstream DNS servers that will handle most DNS queries – I have provided Google's DNS server of *8.8.8.8*. Finally, log DNS queries and DHCP requests – this just makes it easier to check everything is working.

We also want to create a file *fakehosts.conf* to allow us to spoof certain DNS requests:

```
1 10.0.0.9 neohub.co.uk
```

This will cause the *dnsmasq* DNS server to respond with *10.0.0.9* to any request for *neohub.co.uk*.

We then need to bring *dnsmasq* up. I want it to run with output to stderr, so this is done as follows:

```
dnsmasq -C dnsmasq.conf -H fakehosts.conf -d
```

5. Configure and run hostapd

Next, we need to get our wireless adapter to run as a access point.

hostapd allows us to do this.

Install *hostapd:*

```
apt-get install hostapd
```

Create a config file *hostapd.conf:*

```
interface=wlan3
driver=nl80211
ssid=Kali-MITM
channel=1
```

Again – really simple. Use our additional wireless adapter *wlan3* with the nl80211 drivers (which seem to cover pretty much all modern adapters than can be APs), set the SSID to *Kali-MITM* and set the channel to 1. There is no encryption etc. but I really don't need or want it for sniffing traffic.

Then start *hostapd*:

```
root@kali:~# hostapd ./hostapd.conf
Configuration file: ./hostapd.conf
Failed to update rate sets in kernel module
Using interface wlan3 with hwaddr c0:4a:00:1e:64:fd
```

6. Setup routing for the access point

You want a very simple setup at the moment – act as a basic NAT gateway between *wlan3* and *wlan0*.

Without going into any detail, the following commands will set this up:

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo iptables -P FORWARD ACCEPT
sudo iptables --table nat -A POSTROUTING -o wlan0 -
```

At this stage, you should now be able to connect to *Kali-MITM*, get an IP address, and start using the Internet.

Share this:

Twitter Facebook 3 Reddit

THIS ENTRY WAS POSTED IN SECURITY. BOOKMARK THE PERMALINK.

8 thoughts on “Quick and easy fake WiFi access point in Kali”

DanBUK PERMALINK · REPLY
FEBRUARY 4, 2015 AT 12:50AM

Isn’t this just how to setup a WiFi AP?

For this to be ‘fake’ one would be attempting to fool someone into connecting. Maybe even going as far as patching hostapd to run encrypted so as to not alert the client machine they are connecting to an insecure network by accepting any PSK generated handshake yet on the SSID (I forget E/BSSID at this time) that matches ones target network.

Sorry, it is a nice descriptive post but doesn’t fill my boots based upon the title.

cybergibbons PERMALINK · REPLY
FEBRUARY 4, 2015 AT 7:21AM

I guess that is a fair comment.

I’m going to do another ab

setting up Burp proxy and using iptables to redirect traffic to it to sniff https traffic.

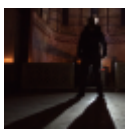
Nayc PERMALINK · REPLY
JUNE 25, 2015 AT 8:12PM

I keep getting:
hostapd failed to update rate sets in kernel using adapter: Alfa AWUSO36NH

With this error I notice victim can never connect to the fake network, never associates an IP.

Using adapter Netgear WG111 v2 everything works great.

So it seems Linset does not like my Alfa AWUSO36NH for some reason although I have watched videos with people using it ? Any ideas?



cybergibbons PERMALINK · REPLY
JUNE 29, 2015 AT 9:07AM

Hmm – I have seen this before when using my Alfa. I think there might be a few version of the chipset, but not sure.

Hackfree PERMALINK · REPLY
DECEMBER 5, 2015 AT 8:52AM

Thank you for the great tutorial…I have Lenovo B590 with 2 wireless cards TL 722N and BCM43142.This works for them but I first had to kill network-manager proces

start hostapd (otherwise it wont start)

federgb PERMALINK · REPLY
MARCH 27, 2016 AT 2:40AM

Hi, i want do something like android`s netspoof options but for ubuntu… netspoof is very easy and 100% dangerous…

rf2632 PERMALINK · REPLY
NOVEMBER 2, 2016 AT 7:11PM

Hi, thank you for this post! I have only one problem: the client cannot get an IP address, it says “Obtaining IP address…” and it wont do anything. I am trying to connect it with an android mobile phone.

Could it be that you give 10.0. class IP while my network has 192.168 class IP?

Thanks!

husnain PERMALINK · REPLY
DECEMBER 8, 2016 AT 6:24AM

in need to install hostpd on my amd kali 64bit please guid me to right way to do so please!

Leave a Reply

Your email will not be published. Name and Email fields are required.

Privacy & Cookies Policy

Comment

Name | Email | Website

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.
