

Forum:[Hack Forums](#)

Thread: [\[tut\] simple tut for anyone wanting to start pentesting/hacking wifi networks \[tut\]](#)

think_alien - April 30, 2011, 2:25 am

1st get yourself a good wireless card:

1. best ive found

name:High Power USB-Yagi Plug and Play directional WiFi Antenna

price:\$120/£72

range: 4km / 2.48miles

dBm:+35

power:2200mw

wireless technology: b/g/n

max speed: 300mbps

chipset:ralink rt2870/3070

link: <http://www.amazon.com/USB-Yagi-directional-Antenna-802-11n-2200mW/dp/B003LLS5JI>

2.often suggested cheaper card

name:Alfa AWUS036H

price:\$34/£21

dBi:5

power:1000mw

wireless technology:b/g

max speed:54mbps

chipset:RTL8187L

link: <http://www.amazon.com/Alfa-AWUS036H-802-11b-Wireless-network/dp/B002WCEWU8>

2nd:

go online and download backtrack linux is is the operating system you will be using to pentest/hack wifi networks

download link:<http://www.backtrack-linux.org/downloads/>

live dvd: burn to cd at 4x

vm:<http://www.virtualbox.org/wiki/Downloads>

3rd:

go to ~Middle's thread where you will find very detailed tut's on wireless hacking

link:<https://hackforums.net/showthread.php?tid=1082349>

~Middle also provides a very nice wpa dictionary can be found at above link or this link

link:<https://hackforums.net/showthread.php?tid=1046679>

Middle - April 30, 2011, 3:14 am

Thanks for trying but:

<https://hackforums.net/showthread.php?tid=1221603>

n0Tolerance1 - May 4, 2019, 7:10 am

Thanks Bro. Appreciated ??

pasnger57 - May 4, 2019, 7:41 am

(Apr 30, 2011 02:25 AM)think_alien Wrote: [\[CITE\]](#) 1st get yourself a good wireless card:

1. best ive found

name:High Power USB-Yagi Plug and Play directional WiFi Antenna

price:\$120/£72

range: 4km / 2.48miles

dBm:+35

power:2200mw

wireless technology: b/g/n

max speed: 300mbps

chipset:ralink rt2870/3070

link: <http://www.amazon.com/USB-Yagi-directional-Antenna-802-11n-2200mW/dp/B003LLS5JI>

2.often suggested cheaper card

name:Alfa AWUS036H

price:\$34/£21

dBm:5

power:1000mw

wireless technology:b/g

max speed:54mbps

chipset:RTL8187L

link: <http://www.amazon.com/Alfa-AWUS036H-802-11b-Wireless-network/dp/B002WCEWU8>

2nd:

go online and download backtrack linux is is the operating system you will be using to pentest/hack wifi networks

download link:<http://www.backtrack-linux.org/downloads/>

live dvd: burn to cd at 4x

vm:<http://www.virtualbox.org/wiki/Downloads>

3rd:

go to ~Middle's thread where you will find very detailed tut's on wireless hacking

link:<https://hackforums.net/showthread.php?tid=1082349>

~Middle also provides a very nice wpa dictionary can be found at above link or this link

link:<https://hackforums.net/showthread.php?tid=1046679>

ok nice but i love you use just suggested very outdated and old OS that is now evolved to kali and the ida of burning a CD up at this time is next to laffable (usb boot devices) save a lot of hassle time \$

TxRx - May 4, 2019, 10:32 am

That setup is WAY overpriced for the flexibility that it will give you...

First of all, the antenna and wireless card you are suggesting are a single unit attached.

When it comes to hacking signals, you're going to need an adapter with an external RP-SMA connector which will allow you to swap and modify your hardware setup according to your needs and your target. One example of this is my thread:

<https://hackforums.net/showthread.php?tid=5963265>

I choose to have the option to switch between smaller rubber duck antennas or even up to yagi or parabolic grids. Also, theres way better versions than the AWUS036H (which only supports a/b/g),

like for example... the AWUS036NHA, or the TL-WN722N and these are way cheaper and supports all the newer technologies.

Also, nowadays you could emulate kali linux (which is the top OS when it comes to pentesting) into any device pretty much. I made a kali pi box with a raspberry pi, which i can carry around discretely and access from SSH from my android phone.