

Forum:[Hack Forums](#)

Thread: [Legion | Learning to hack wireless 101](#)

HackRain - May 13, 2013, 2:22 am

[img]http://i.minus.com/ieq6viOQ6szdE.gif[/img]

Learning to Hack wireless at first can be a bit daunting,
You may find yourself lost and confused about how to implement the attacks, or how to even start.

In this thread, I will be giving you all the necessary information needed to start your wireless adventures.

Presuming you are aware of what wireless is, then that it all the information you require to move on and start reading.

Note: this has been written in a way you can read threw start to finish, as well as use for reference.

prerequisites.Spoiler ([Click to View](#))

You will need the following:A wireless card cable of packet injection

A linux operating system.

Lets talk about these pre requisites.

The big question, what is a wireless card and what is packet injection?

A wireless card is an adapter used to connect to wireless networks.

Most laptop's now days come with built in wireless cards.

If your a desktop owner, then you may have a PCI wireless card.

How ever, I strongly recommend you buy a USB compatible wireless adapter. I will speak more about this later.

So that leaves the packet injection.

Packet injection can be commonly looked at as:

"the ability to force insert malicious data into a wirelesses network"

As you can see, this is crucial. We will need to insert malicious data into the infrastructure to gain results.

This is why packet injection is a must.

Whats a good wireless card?

Does it support injection?Spoiler ([Click to View](#))

Well a good wireless card in terms of hacking, is preferably a USB adapter, with a replaceable/upgradable antenna.

The USB card is a mandatory, to come with packet injection.

The reasoning behind having a USB wireless card, rather than an inbuilt one or a PCI one, is simple.

the first reason would be that a USB wireless card swill be welcomed by Virtual machines, unlike on board wireless cards.

this means if you desire, you can run your linux operating system in a virtual machine.

The second reason, would be portability.

The ability to take your wireless card where ever you go and a copy of backtrack on your thumb-drive.. think of the possibilities.

Now, Why should it have a removable antenna?

Well, this is not mandatory, in fact, this is just icing on the cake.

A few weeks down the track, when your a WIFOO master, you may want to adventure with your wireless capabilities.

With a customizable antenna, you will be able to remove your 5-9 dbi small antenna, and purchase a HUGE high gain antenna for your roof.

This could potentially mean you can connect to not only neighbors, but also hit coverage up to 20-30kms away!

Like i said, icing on the cake.

Now, for a cheap reliable wireless card:

[ALFA AWUS036NHA](#)

This card is cheap as chips, and comes with EVERYTHING i have mentioned above. You cant go wrong.

This card is used by a large amount of members here, and is highly supported/recommended.

How can i test if my card supports packet injection?Spoiler ([Click to View](#))

Firstly, if your not already aware of the aircrack suite, and you do NOT have it installed, come back to the question at the end of the reading.

To test if your card is capable if packet injection

simply open a terminal and type

Code airmon-ng start wlan0then

Code aireplay-ng -9 mon0If you get:

Quote:"injection is working!"

then you are all in the clear to start.

If not, buy this card:

[ALFA AWUS036NHA](#)

Test lab installationSpoiler ([Click to View](#))

Okay so you have a wireless card, and it may or may not be supported. Thats okay, lets get Linux installed so you can

test it out, and continue with the tutorial.

The first decision you may face is, "what operating system should i install"

Well, im going to give you two choices for the sake of this tutorial.

You can install:

Ubuntu 10.04 LTS

or

Backtrack 5r3

Other operating systems MIGHT work, but i have not tested all of them, and I'm giving you the safest most plausible route here.

Ubuntu would be the choice of preference for a die hard hacker, if you want to get to know linux, and you dont mind some extra playing around, then go for this!

I myself started with ubuntu, At first it may be a little more confusing, but it is much more beneficial in the long run. You will learn to not only hack wireless, but you will learn how to use a real linux distro also!

Backtrack, this choice is for those who "just want it to work" backtrack comes on board with ALL of the tools required to do practically anything in the wireless world, and sum.

This linux distribution was made to be a hacking OS, it was built of ubuntu 10.04 kernal, but with the addition to coming with pre installed, pre patched software.

This Operating system how ever, is not suitable to use as an every day operating system.

How to install Ubuntu

Spoiler ([Click to View](#))

First off, if you dont want Ubuntu, and you prefer to install back track. skip this reading and close the spoiler.

The next spoiler section is suitable for you.

You have two options here.

You can install it in a virtual machine environment.

or, you can install it side by side with windows.

Note: Side by side installation, simply means to install it on the same hard drive as windows. this will meen when you boot your pc, you can choose weather you want to open windows, or ubuntu.

remember, if you install it with a virtual machine, then you will DEFINANTLY need a usb wireless card, no if's or but's.

To install ubuntu you will first need to download the ISO image of ubuntu:

<http://releases.ubuntu.com/lucid/>

Choose 32 bit if your using a 32 bit , and 64bit if your running 64bit respectively.

to install ubuntu on a virtual machine follow this tutorial:

[This tutorial](#)

To install it side by side with your Windows operating system, follow this tutorial:

[This tutorial](#)

Note: you will need a spare USB drive of at least 4 gig of memory.

How to install Backtrack

Spoiler ([Click to View](#))

If you would rather install ubuntu, close this spoiler and follow the guide above this one.

Installing back track is next to identical to installing ubuntu.

you have the option of a side by side installation
or, a virtual machine installation.

* Installing in side a virtual machine, means you can use windows and linux the same time, you will be able to minimize linux and still continue doing every day tasks in windows.

The down side is, you will have to purchase a USB wireless card.

*Installing it side by side with windows, this means upon booting your PC, you will be prompted with the option "boot windows, or boot backtrack". Backtrack will be stored on your hard drive, just like windows. The up side to this installation, is backtrack will utilize your CPU, GPU, and RAM.. Meaning a much quicker environment.

To install backtrack in a VM, follow this tut:

[This tut](#)

To install backtrack side by side (Dual boot), follow this tut:

[This Tutorial](#)

How to actually hack wireless

Spoiler ([Click to View](#))

From here,everything is set up and ready. you will need to boot up your linux OS and scan for wireless around you.

To do this, just just which wireless is in range.

Simple simple.

After you find a strong wireless signal, look at the encryption type. It will say either WPA, WPA2 or WEP

This is important, as this will define the rest of you hacking.
You need to learn how to identify a wireless security.

its not hard no, but it must be done.

So after you have found your victims security type, all you have to do is follow one of the guides in the stickie thread relevant.

For instance,

If your victim has WPA2 security, you will need to follow a tutorial on hacking WPA2. which can be found in this thread:

[THIS THREAD](#)

If they are using WEP, then respectively, follow the tutorial on hacking WEP, also found here:

[THIS THREAD](#)

FYI: that thread contains all the necessary information to start your wireless rampage.

Note: im not going to try to fit every tutorial on hacking wireless in here, this is just a guideline for you to be "fail-proof"

How to change your mac address

Spoiler ([Click to View](#))

simply follow my other tutorial found here:

[HERE](#)

kray - May 13, 2013, 2:24 am

Solid directory of tutorials. Several tutorials written into one page, HQ.

HackRain - May 13, 2013, 2:26 am

It was more a follow along.

If you're new here and have no idea, then this will guide you threw.

TheGrayAviator - May 13, 2013, 2:47 am

(May 13, 2013 02:26 AM)?PandaSec Wrote: [\[CITE\]](#) It was more a follow along.

If you're new here and have no idea, then this will guide you threw.

Now if you can't follow this tutorial, then you shouldn't attempt hacking at all.

Great tutorial as always HQ.

PoisonKnife - May 13, 2013, 2:49 am

Thanks for this tutorial. I have bookmarked it and will try it later today.

Amazing work!

HackRain - May 13, 2013, 3:54 am

Thanks guys.

I appreciate the kind replies.

PinkPanther - May 13, 2013, 9:09 am

If you're new to wireless hacking, this guide will get you up to speed.

Great stuff ?PandaSec.

serkoulik - May 14, 2013, 10:04 am

First steps of Wireless hacking...nice PandaSec.

TheCyb3rAlpha - May 15, 2013, 8:46 pm

Great tutorial mate !!

it would really help newbies to learn about wireless. SOLID HQ !!

MomoChan - May 17, 2013, 5:06 am

lol I still need to get the first bit, but when I do I will definitely try it :)

The Commander - May 17, 2013, 5:08 am

Great thread solid work here! Legion #1

HackRain - May 17, 2013, 6:01 am

Thank you kind sir.

More to come in the close future.

n0tion808 - May 24, 2013, 3:26 pm

question: you mentioned ubuntu 10.04 instead of the current release, why? just out of curiosity, great tutorial btw

HackRain - May 25, 2013, 12:16 am

(May 24, 2013 03:26 PM)n0tion808 Wrote: [\[CITE\]](#) question: you mentioned ubuntu 10.04 instead of the current release, why? just out of curiosity, great tutorial btw

I've had it tested and working on 10.04, the majority of tutorials for patches and fixes for wireless cards are written for 10.04.

I've tried unity (the latest) and i found it to be less stable for wireless pentesting.

If you're a bit linux savy then choose your own distro, but i recommend if you're a beginner, to go ahead and just use my prerequisite suggestions.

loco1 - June 30, 2013, 8:00 pm

need some help: i have windows vista, can this be done with vista and win xp ?

please reply thanks

TheGrayAviator - June 30, 2013, 8:56 pm

(Jun 30, 2013 08:00 PM)loco1 Wrote: [\[CITE\]](#) need some help: i have windows vista, can this be done with vista and win xp ?

please reply thanks

Yes it can be done in Windows, but it's a very painful process that I would not recommend to you, unless you like frustration.

And this Hack Wireless 101 guide, requires you to use Backtrack and NOT Windows.

RS_Smuggle - June 30, 2013, 9:56 pm

Thanks appreciate the tutorial :). (35 char block bypass) lol