***** This tutorial was released on April 2020, copied from HackTown (hacktownpagdenbb.onion)*****

WI-FI HACKING

Act I of this HackTown cybercriminal series is meant to teach you how to hack other people's Wi-Fi networks so you're able to use them for your devious actions or to enhance your OPSec. You should've already gone through ACT 0 - OPSec before moving forward in this course. Being able to compromise other Wi-Fi networks around you gives you the ability to be even more difficult to locate when someone or something is hunting you down. Why use your own Wi-Fi network when you can be using other people's networks to perform your dark web activities?

All this and more!

If you're looking for more teachings, guidance, mentoring, or know someone who can benefit from these courses consider purchasing a membership at HackTown

There will be points throughout this guide marked in **BLUE**. These points are useful to fully grasp the concepts taught and help with understanding techniques and explanations on various topics. It's important that when you read them you stop and take the time to do what they say or follow up with them. The syntax of code to be typed into Terminal or the command line will be **RED**. So anytime you see something in **RED** you know that it's syntax code and should be entered into Kali, Terminal, Windows command line, etc.

Introduction

This course was written by me, Funshine.

Contact me at:
hacktown@secmail.pro

This course, like every course here at HackTown, is based on my experience when I was operating as a cybercriminal with the techniques, tactics, and procedures I used during my operations. I was a successful cybercriminal who retired many years ago with cashing out the profits I made through cybercrime and enjoying DAT cryptocurrency boom! I,ve been floating around in life for quite some time and having too much time on your hands is never a good thing. Since I've always enjoyed writing I've designed these courses around my experience as a cybercriminal giving you the opportunity to duplicate my tactics, techniques, and procedures to experience financial freedom for yourself.

First off there is no one way of doing things. These courses are not the word of law when it comes to cyber crime but this is from my perspective so if you have something to add, have a better way of explaining things, or anything you think that I don't know that pertains to the topics in these courses send me a god damn email and let me know what is WAT. That way we can keep it all updated for everyone to enjoy and cause a fuck show in their hometowns. HackTown will arm you with the right information on cyber warfare which is exactly what you're wanting to learn. Good job my friend you found this place.

This course is meant to teach you how to hack Wi-Fi networks for your own personal gain and to ensure you're not using your own Wi-Fi network when you're doing questionable shit online. This is another important skill to learn when beginning out with your cybercriminal career. Hopefully you can take away many useful points that you're able to incorporate into your daily mayhem causing activities.

It's assumed you have general knowledge of hacker techniques, lingo, interests, and terminology that is used in this course. This document has been reviewed however there may be some language and grammatical errors as translation sometimes get misunderstand. If you come across errors (spelling or grammar) or have more information that you think can be added please let me know.

Lastly, this course does not include EVERYTHING for you. Honestly how could it? It's expected that you're capable of doing some research on your own as well. These teachings will show you how to stay and remain hidden but you cannot be expected to be spoon fed with hand holding along the way. Google is your friend. Any question, problem, or error paste it directly into Google and read through forums, blogs, etc. until you find your answer. If you're not capable of this then please stop now before you hurt yourself. You may think this is a cop out but most, if not all, of your questions can be answered this way and realistically the amount of questions you'll have will be vast so it's best to get efficient in searching and finding your answers on your own.

Being able to effectively search, read, learn, and find your answer is a skill on its own so be

prepared to be somewhat self-sufficient when learning new material. Most people who are good at hacking, carding, etc. have learned step by step from books, others, or whatever means neccessary to get that knowledge so treat this like a University or College course and do some homework and read, read, and read some more. If you have major problems following this course and cannot replicate the teachings then what you're attempting to do and learn is way beyond your capabilities and you should stop what you're doing, accept your fate, and focus on something easier such as cabinet making, cake baking, or watching the world pass you by.

Alright then you crazy mother fuckers, let's get into it shall we!

Required Wi-Fi hacking hardware

Everyone uses a variety of hardware to hack into Wi-Fi networks with slight variations from setup to setup. There's no "right" way to have your gear setup but I recommend getting a backpack that can house all your Wi-Fi hacking gear in one place and keep the antennas hidden.

You want to blend in while you're sitting at the coffee shop hacking the Wi-Fi network across the street.

What do you think of Russian hackers or the Federal Security Service (FSB) abilities? Russian, Iran, North Korea, and many others have agents around the world conducting cyber operations against whomever all the time. We all have our own way of doing things but learning from "professionals" does help when trying to figure out how you want to operate.

Click to read - Learn about the Russians Wi-Fi hacking busts

It's a good idea to keep in the know (FaceBook, Twitter, Instagram, etc.) of other nation state actors and what they're up to so you're able to replicate what other government level hackers are currently doing and copy their methods for your own needs.

Important:
The Wi-Fi network cards recommended in this course require your laptop/computer to have USB 2.0 or a USB 3.0 port. Check your laptop/computer specifications to ensure they meet these requirements but most modern day laptop/computers will have these ports.

When you get more experience hacking Wi-Fi networks you can invest more money into a larger setup should you choose to go fucking crazy.

For now, <u>you will need the following:</u>

- **(2) wireless cards capable of packet injection.**
- **Wi-Fi antennas (not needed right away but a must for the future)**
  Many people get confused about which network card they should purchase so I'll make some recommendations so you don't have to figure that shit out on your own.

  Head over to https://www.alfa.com.tw/service_1/all/1.htm and purchase the Alfa "AWUS036NH" or "AWUS036ACH" network card(s). You can also purchase these cards from Amazon, Ebay, Alibaba, and any other major online retailor.

  Whichever Wi-Fi network cards you choose make sure you always have (2) of them to maximize chance of success!

  Below is the Alfa **AWUS036NH** 2.4GHz single band network card.

The picture below is the Alfa **AWUS036ACH** Dual Band 2.4GHz and 5GHz network card.

Later on in your "career" it's recommended to pick up a wide variety of antennas. Depending on what your goals are you might want a magnitude of Wi-Fi networks to be able to connect to. Antennas help you increase your range of connectivity allowing you to connect to a Wi-Fi network a block away, the next apartment, or in some cases up to a 1/4 mile away.

When you're looking at purchasing different antennas there are a few things you need to know.

A bigger antenna like a 15dBi or 20dBi doesn't necessarily mean it's better than a 2dBi per

se. A 2dBi antenna is very effective at a short range whereas a 9dBi antenna is not effective at short range but works well with picking up signals from a distance. Also, if there are walls or other barriers between you and the Wi-Fi network you're trying to access a larger antenna will not make the signal better.

Let's say you want to connect to your neighbors Wi-Fi network across the street from you then a 7dBi or 9dBi antenna would be much better in this situation. The 7dBi-9dBi antenna isn't that big and is easily concealable in a shoulder bag or backpack that gives good range. Eventually you'll be wanting other antennas to increase your Wi-Fi connection range such as outdoor antennas and parabolic antennas. The stock antenna that comes with the Alfa network card that you'll purchase for this course will suffice. These antennas look like:

"Yagi" antennas are known for connecting to a Wi-Fi network from a distance and are widely used in the hacker community. These are best suited when targeting a Wi-Fi network from a great distance. They generally look like:

Parabolic antennas have great range but are very specific and can be annoying when trying to figure out the best angle to get the best signal. Picture using these antennas like using a laser pointer. The beam of light from a laser pointer is so small but extends for a long distance however, can be tricky when targeting a small area far away. My advice here is that hopefully you're in a densely populated urban area and live higher than most buildings around you. If possible aim it directly at a high story building (ideally through a window) that's fully populated so you can compromise Wi-Fi networks up to a mile away. If you purchase a directional antenna then you can use the same techniques a hacker used to attack the Wi-Fi network of a popular organization sitting in his car from the parking lot which you'll learn about in the next article below. Ideally you would have a directional/parabolic antenna mounted on your balcony or outside facing a densely populated building or towards a known free Wi-Fi network. A parabolic antenna looks like:

Open the link below and search for "war driving" on the page (CTRL+F) and read that paragraph. When you have finished the paragraph read the whole article from the beginning.

Click to Read - The Great CyberHeist

As you can see antennas can be used in a wide array of possibilities when it comes to hacking. This is why it's important to have your gear setup in a way that is portable, concealable, and will accomplish what you're trying to do. Are you aiming your antenna at a local restaurant in order to compromise their network and siphon POS credit cards from memory over their network? It's best to do this from a distance.

If you do purchase a better antenna try and conceal it as best you can because having antennas sticking out of every pocket you have while at a coffee shop isn't really "blending" in now is it? Imagine someone thinking something was peculiar about their internet connection at a public Wi-Fi and seeing someone with strange antennas, stickers on their laptop, wearing a top hat, and looking up to no good sitting there. It's just not good. Blend in. Keep your laptop clean looking, keep professional, and appear to be a normal plain user sitting in a coffee shop not up to anything. No need for "I love H4X0R5" stickers on your

laptop. Keep average looking and don't talk to anyone about your activities. A wolf in sheep's clothing. Have the cables running right into your backpack/bag close to your computer if you have USB cables.

Remember, those fucking Russians had their whole car setup for Wi-Fi hacking! Be creative but stay concealed.

Now that you're educated on the gear you need and have ordered the Alfa Wi-Fi network cards we can now start hacking Wi-Fi networks. When you have the right gear you can continue onto the next chapter.

Pre-requisites

The syntax of code to be typed into Terminal or the command line will be **RED**. So anytime you see something in **RED** you know that it's syntax code and should be entered into Kali, Terminal, Windows command line, etc.

It's best to have (2) network cards capable of injection.

Computer/Laptop

- Intel or AMD CPU
- Minimum 4GB of RAM
- 60+ GB of hard disk space
- Internet access
- Kali VM
- (2) External Wi-Fi network cards and antennas

The more memory your computer has the better it will be because being able to run multiple VM's at once is very beneficial. When you run VM's you dedicated some RAM to those machines and operating smoothly is what everyone wants. Hard drive space is important too if you plan on having a multiple VM's as each can take up to 10GB each minimum.

"Professional" cybercriminal maniacs have their machines like:

- Intel or AMD CPU
- 32+ GB of RAM
- 1 TB+ of hard disk space
- Internet access
- Kali VM
- (2) External Wi-Fi network cards and antennas

Download VirtualBox and the VirtualBox Extension Pack from:

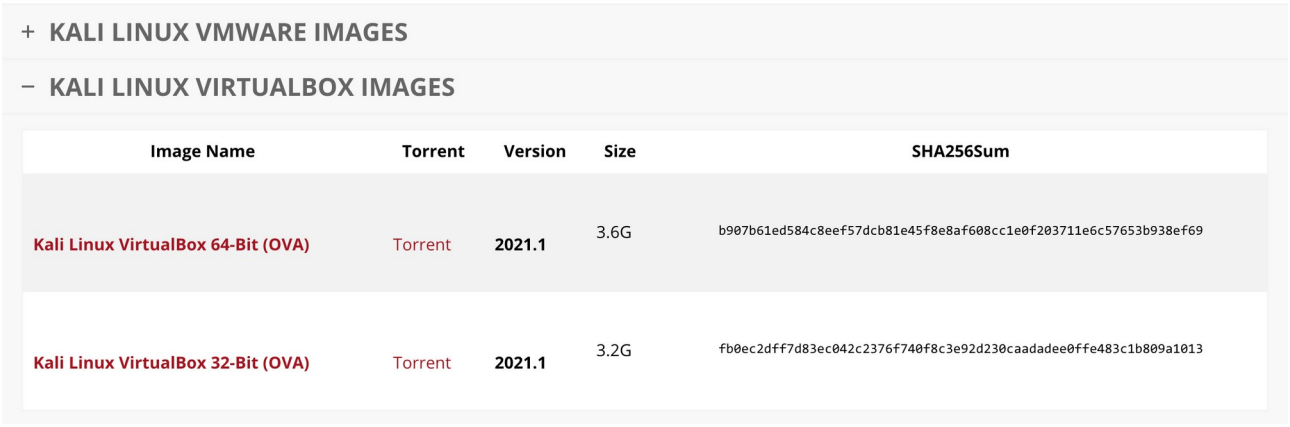
https://www.virtualbox.org/wiki/Downloads

Download Kali VirtualBox

https://www.kali.org/downloads/

Make sure you select the VirtualBox image and not the VMWare image!

https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download



+ KALI LINUX VMWARE IMAGES

− KALI LINUX VIRTUALBOX IMAGES

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux VirtualBox 64-Bit (OVA)	Torrent	2021.1	3.6G	b907b61ed584c8eef57dcb81e45f8e8af608cc1e0f203711e6c57653b938ef69
Kali Linux VirtualBox 32-Bit (OVA)	Torrent	2021.1	3.2G	fb0ec2dff7d83ec042c2376f740f8c3e92d230caadadee0ffe483c1b809a1013

Download either the 64-Bit or 32-Bit version of Kali. This is different for everyone so if the one you downloaded doesn't load Kali then the other one will and now you'll know! ;) If Kali boots up and you're at the Kali desktop then good!

If you can't run any of those VirtualBox files then you can try and download the .iso file and create a new VM that way. If those ways don't work I'm afraid your computer just isn't up to par sisters and brothers.

Default Kali username and password is "kali".

OK this is the part that will differ for people depending on which network card you purchased.

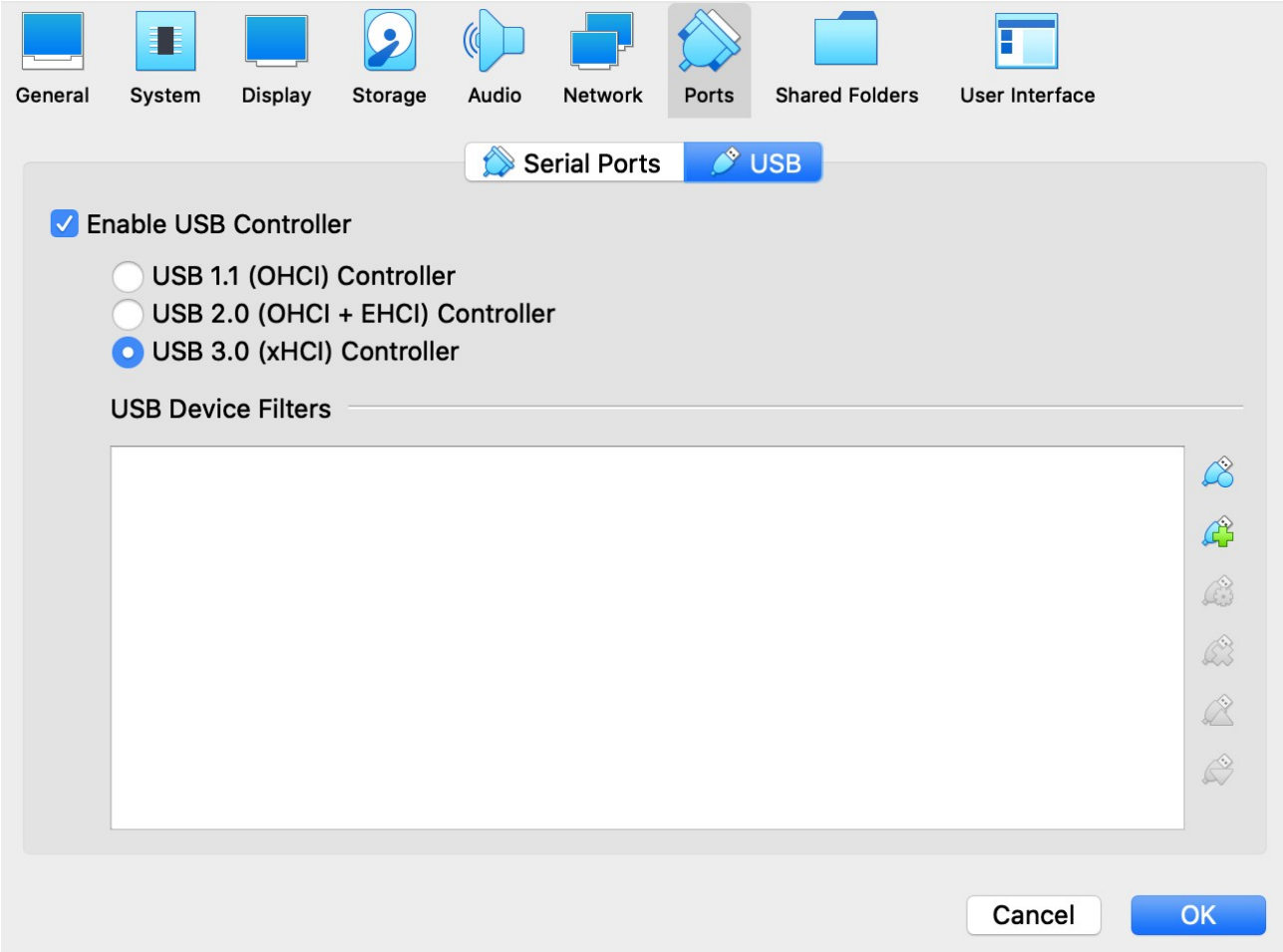
Click HERE if you purchased the **AWUS036NH** network card.

Click HERE if you purchased the **AWUS036ACH** network card.

Click HERE if you already know your network card is capable of injection or want to continue.

AWUS036NH network card setup instructions.

- Shutdown Kali.
- Plug in your Alfa AWUS036NH into a USB slot.
- In VirtualBox click Settings - Ports - USB - "Enable USB Controller" on USB 3.0 then click "OK".



- Re-launch Kali.

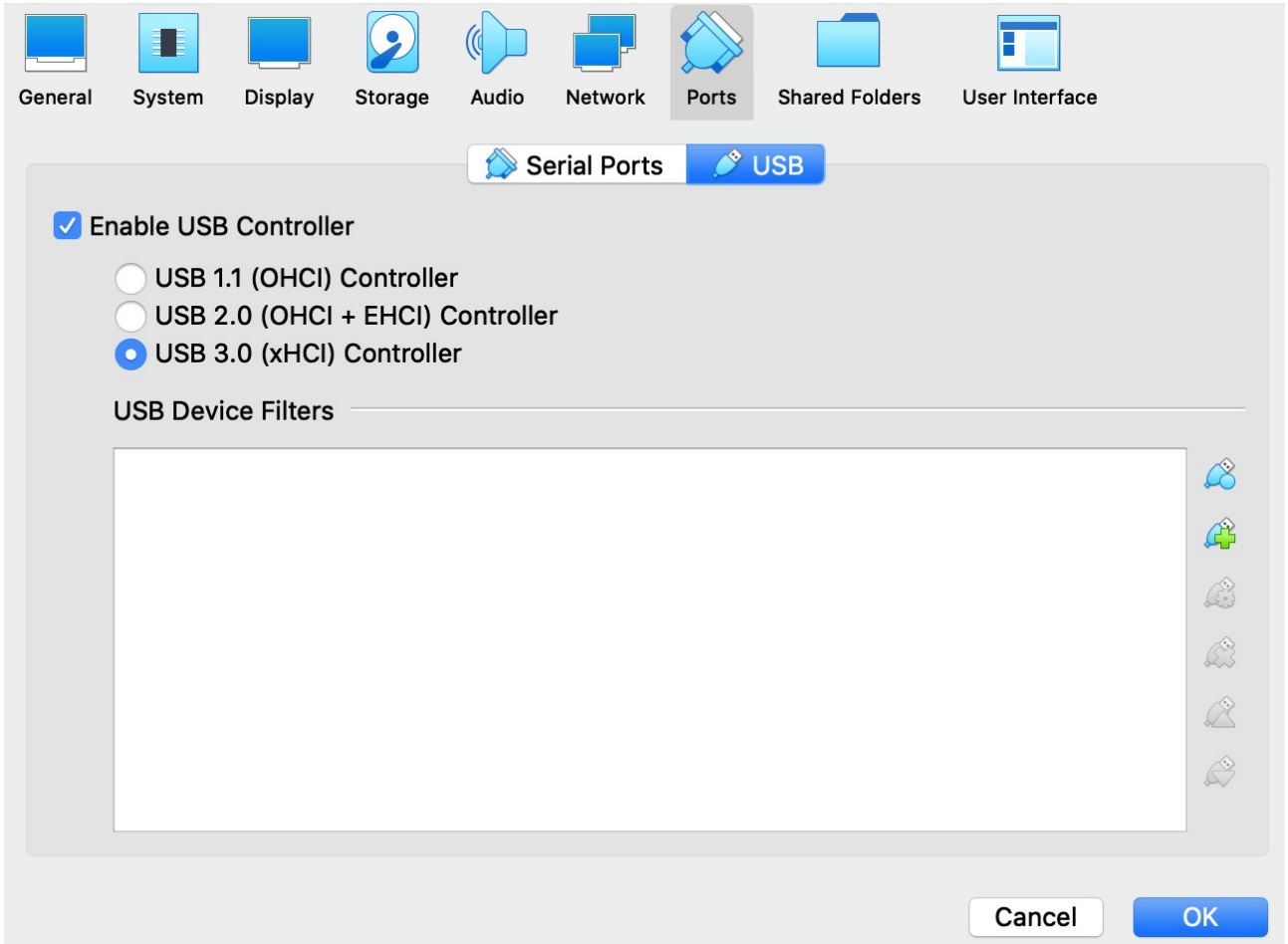
  Once Kali starts and you're presented the Kali Desktop click on "Devices" then "USB" and finally select the "Realtek 802.11n NIC" adaptor to attach the Alfa network card to your Kali VM. You will have to attach your Alfa network card each time you plug it in to use it.

  Your Alfa network card is properly installed and ready to cause chaos.

  When that's complete click HERE to continue.

AWUS036ACH network card setup instructions.

- Shutdown Kali then select the Kali VM in VirtualBox and click - Settings - Ports - Select "Enable USB Controller" on USB 3.0 and then click "Ok"



- Re-launch Kali

  If you purchased the AWUS036ACH you may need install the drivers in Kali to get it working.

  To do this type the following into Kali in Terminal:
  sudo apt-get update
  sudo apt-get install realtek-rtl88xxau-dkms -y
  sudo shutdown -r now

  Your network card is properly installed and ready to cause chaos. Load up your Kali VM and then click on "Devices" then "USB" and finally select adaptor to attach the Alfa network card to your Kali VM. You will have to attach your Alfa network card each time you plug it in to use it.

  Your Alfa network card is properly installed and ready to cause havoc so click HERE to continue.

  Continuing on....

If you encounter an issue with your USBs and Kali won't start without an error this is most likely because you don't have a USB 2.0 or 3.0 port. Make sure your Alfa card is plugged in and attached to your Kali VM with USB 3.0 settings. If you do not have a USB 3.0 port on your laptop you won't be able to use the Alfa network cards recommended in this course and will not be able to continue.

Upgrade your shit ladies and gentlemans.

Next we need to setup our Kali machine.

Ensure you're connected to the internet on your host machine and open Terminal in Kali VM. If you don't know where the Terminal is then search for it using the search function in Kali.

The newst version of VirtualBox and Kali make it so you're able to copy text from your host OS and paste it directly into Kali Terminal. This way you don't make silly mistakes when copying the syntax out. Copy all the syntax and paste it into Terminal for ease and if you can't do this then install the VirtualBox Guest Additions which is a simple Google search away.

Open a new Terminal and type:
sudo apt-get update && sudo apt-get dist-upgrade -y && sudo apt-get install vsftpd lighttpd isc-dhcp-server hostapd-wpe dnsmasq hcxtools pkg-config libcurl4-openssl-dev libnl-3-dev hostapd zlib1g-dev libnl-genl-3-dev libssl-dev leafpad python3-pip -y && sudo apt autoremove -y

If you get any errors at all when running the above command such as:
"E: Could not get lock ...."
Then run these commands before running the above command again:
sudo rm /var/lib/dpkg/lock-frontend
sudo rm /var/lib/dpkg/lock
sudo rm /var/cache/apt/archives/lock
Once you've run those commands you can the run the above update command with success.

If you encounter the screenshot below hit spacebar on your keyboard to select "/dev/sda - VBOX_HARDDISK" and hit enter.

Once that's done run the following commands in Terminal:

git clone https://github.com/wifiphisher/wifiphisher.git
cd wifiphisher
sudo python3 setup.py install
cd ..
sudo git clone https://github.com/ZerBea/hcxdumptool.git
cd hcxdumptool
sudo make
sudo make install
cd ..
sudo rm -r hcxdumptool
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

If you're interested in furthering your "hacker" knowledge you should begin to research Kali Linux and the programs on it. Don't get overwhelmed by the amount of tools available to you in Kali and your lack of knowledge surrounding them but try and stay focused on what interests you. Becoming a hacker or cybercriminal takes time and requires you to

learn just like others before you have step by step.

Just relax and try to know the basics. Once you have the basics down you can move forward because if you don't take it slow you'll be overwhelmed and frustrated with the vast amount of information you'll be presented with.

Remember, it's not going to happen overnight and by learning how to increase your OPSec along with how to compromise Wi-Fi networks is an important step to remaining out of trouble so let's just focus on that for now.

Hacking Wi-Fi Networks
Instead of me explaining every technical detail about WEP, WPS, and WPA/WPA2 WiFi networks I'll direct you to an excellent resource as this topic has been explained, literally to death, across many hacker forums on the internet.

However, most of the Wi-Fi hacking information out there on the internet is outdated or people just don't know what they're talking about which can lead to confusion when trying to learn this shit. Furthermore Kali has been updated and some syntax that is floating around on hacker forums no longer works which bogs people down in misinformation land. If I'm part of a group or forum and I see "How do I hack Wi-Fi networks?" posted I literally shit my pants in disbelief. Specially on a darknet hacking forum. Like how the fuck did you get here?

Wi-Fi hacking is one of the most annoying topics to answer in the forums but that being said getting everything to work properly is always a hurdle for many people out there which I take for granted. Having the right information that is up to date is something to be said so I've linked very helpful videos for you. Now keep in mind most of the stuff talked about on the videos will work (WEP and WPA/WPA2 attacks) except a few items but the point of watching the videos is to learn all the technacalities of Wi-Fi hacking for those wanting to know it all.

Click below to watch the Wi-Fi hacking megaprimer on YouTube and watch up to Part 26. You can follow along with the SecurityTube Megaprimer if you'd like but please note some attacks are outdated.

Click for Videos

You should have already purchased the required Wi-Fi hacking equipment explained in the last chapter (network cards and optional associated antennas) to continue with this course. If you haven't purchased the required items you should do that now because without having the right equipment following along with this chapter is a waste of time and cannot be completed.

Alright let's start.

Open VirtualBox and fire up your Kali VM. Once Kali fully boots up plug in your Alfa network card one at a time into your laptop and once you've plugged them in go to File - Devices - USB adaptor to select the Alfa Wi-Fi network card and ensure it has a check mark beside it to ensure it's connected to the Kali VM so we can use it.

From here on in its assumed you know what WEP, WPA/WPA2, and WPS networks are and their vulnerabilities. As attackers we like to start with the lowest hanging fruit and work our way from there. Finding WEP/WPS networks is fading out due to their insecurities but it's always a good idea to check around for it because you never know!

Recommended Wi-Fi hacking tool

You will need (2) wireless cards (Alfa cards) to maximize the next methods to the fullest. If you only have (1) Alfa network card you'll be limited in what you'll be able to attack.
Make sure you have (2) wireless network cards plugged in and recognized in your Kali VM.

Running "sudo airmon-ng check kill" should be used every time you launch Wi-Fi attacks to ensure there is no other applications that will interfere with our attacks. Good habit to do this every time you plan on hacking a Wi-Fi network.

There's no need to manually put your Wi-Fi network cards into monitor mode as the program discussed below will do it for you if required.

In Kali VM:
sudo airmon-ng check kill
sudo wifite

Select the Wi-Fi network card to use and let the wifite tool run for around 60 seconds. Once that's done hit CTRL+C and select the Wi-Fi network you're wanting to target. It's best to ensure there are clients already associated to the Wi-Fi network you're targeting to cycle through every attack (ie: WPA/WPA2) against it.

wifite uses a default wordlist when cracking the 4-way handshake but you can specify which wordlist to use. The default wordlist is a good place to start.

A nice feature of the wifite tool is instead of specifically targeting one Wi-Fi network you can tell wifite to attack "all" Wi-Fi networks in the area around you. Since this tool is automated you could kick back and do other things while wifite works in the background and goes after all the lowest hanging fruit around you. Very nice! Get high!

Any hotel you stay at, coffee house you sit at, friends place you go to, or anywhere you have a potential to use an internet connection you should try hacking into every Wi-Fi network around you possible so you have multiple networks you can use when online causing fucking havoc. Do this because you want to have multiple Wi-Fi networks that you can use for your own needs. The more Wi-Fi networks you have access to the better. Once you begin to add more and more Wi-Fi networks that you have taken over to your list you can start to use each Wi-Fi network at different dates and times. If you live in a dense urban area it's best to have 50+ Wi-Fi networks and use a different one each day, every other day, etc. Before you know it you'll be able to log into a Wi-Fi network that you won't be logging into again for well over 2 months. Constantly changing locations and Wi-Fi networks for your "business" activities makes you very difficult to locate if someone is onto your activities. Keep mobile.

Also, when you continue on to the next course the more Wi-Fi networks you hack onto the more targets you have to potentially infect with malware, ransomware, RATs, etc.

Build your Wi-Fi network empire every chance you can! If you travel or constantly move around you can see why this is important, better for your anonymity, and makes you a very difficult target to track. Imagine the time and man power associated into finding and tracking you? The financial costs associated with this means you have to be a target that's worth the time, money, efforts, and worst-case scenario after they try and trace IP after IP they associate you to a geographical area, hacked Wi-Fi network, or a public Wi-Fi. Again, if you move around a lot, travel, or are constantly on the move the better it will be for you.

Now at some point you're going to realize you're not able to crack every Wi-Fi network you come across and not every Wi-Fi network can be cracked or hacked. It depends on a lot of factors like signal strength, location, password complexity, etc.

Signal strength is very important when targeting Wi-Fi networks with success. The physical barriers that are in between you and the target Wi-Fi network can and will interfere with your attacks. Just because you see great signal strength when using these programs sometimes can be misleading so keep an open mind when you see %100 signal strength. If you're unable to launch an attack against a Wi-Fi network it might be because of these reasons such as walls, metal, other radio interferences, objects, etc.

You'll soon find out some passwords you're just unable to crack due to the complexity of them (IE: a password of "12wedsW24#5$ETRgerfsf"). It's very common not being able to crack the WPA/WPA2 password if they've used a proper password to secure it. If you cannot crack it then you'll want to move onto an "Evil Twin attack" to trick the users into entering their WPA/WPA2 password. You'll learn about this in the next chapter.

Now that you understand how to hack Wi-Fi networks go sit in a parking lot with a directional antenna pointed towards a foreign embassy and hack their shit you fucking spy.

If you want to know the older manual way of hacking Wi-Fi networks please click below.

Click to learn older Wi-Fi Hacking techniques
(continue to 2b)

When you're unable to hack a Wi-Fi network
You should always have a basic wordlist that you'll use against the Wi-Fi network you're trying to crack. There are plenty wordlists to use in Kali but there are many more out there to be utilized (a simple Google search away). Once a wordlist has been exhausted it's time to use other resources for cracking the password. It's better to outsource password cracking to online services that can utilize way more CPU/GPU power then you'll want to invest into buying yourself. Ultimately you could setup a separate desktop dedicated to password cracking, but this isn't really necessary or needed today and that's fucking expensive.

Here is a website with many large wordlists should you choose to download and use them.
https://weakpass.com/wordlist

Online WPA/WPA2 cracking services highly recommended:
https://www.onlinehashcrack.com
https://gpuhash.me
https://hashc.co.uk

OK if you've been hacking Wi-Fi networks or just learning how to hack them you'll soon realize that you're unable to hack onto every Wi-Fi network you come across. This means you've tried attacking WEP & WPS, you've run the .cap file with the WPA/WPA2 handshake against every wordlist in your arsenal, and you've used online dedicated services for cracking WPA/WPA2 passwords, and still you're unable to crack the Wi-Fi password. There are times when you'll want and need more networks or want to gain access to a certain network so you'll need to figure out how to get this shit done.

Some people skip to using this method without trying to crack the WPA/WPA2 password because it works without going through a brute force dictionary attack and taking more time then needed. I suggest starting off with passive attacks before actively engaging your target. Think it over.

Remember, the closer you are to the target Wi-Fi network the better chance of success you'll have when launching these attacks. You want to be the best and closet transmitting signal for this attack to properly work. This is very important. So you're either in the same area as the network you're trying to hack with the better antennas OR you have a directional/parabolic aimed directly at the target area. Again, your goal is to be the strongest transmitting powered source around so people connect to you easily.

You will need (2) network cards capable of injection (Alfa network cards or similar) for this attack to work. As you've learned from watching the videos in the Wi-Fi megaprimer you're able to setup your own access point and name it whatever you'd like. If you're targeting "HOME-Wi-Fi" then you would set your rogue AP up to broadcast "HOME-Wi-Fi" as well. One network card will be used to bring up your rogue AP and the other network card will be used to launch a Denial of Service (DoS) attack against the real "HOME-Wi-Fi". The goal with the DoS attack is to overwhelm and take down the real "HOME-Wi-Fi" preventing people from connecting to it while at the same time bringing up your rogue AP

tricking people into connecting to you instead. The victims will think they're connecting to their "HOME-Wi-Fi" network and not realize they are indeed connected directly to you!

When you DoS the Wi-Fi network this will bring down the real "HOME-Wi-Fi" network and will knock everyone offline who's connected to it. The people connected to the "HOME-Wi-Fi" network would eventually notice they do not have internet connection anymore and have been knocked off their Wi-Fi. Wouldn't you notice this? What do you do when you don't have a Wi-Fi connection on your home network? How would you trouble shoot it? In this type of Wi-Fi attack we're targeting the people and not anything to do with technology per se and is know as an EvilTwin attack. We're using social engineering 101 against the Wi-Fi network owners who know the password that we want.

The "average" user is capable of knowing when they do not have a Wi-Fi connection and are capable of trouble shooting a little bit to the best of their ability. They will click and search for their Wi-Fi network or at least troubleshoot a little bit. The goal with an EvilTwin attack is the only Wi-Fi network the people will be able to connect to will be your EvilTwin network which has the same name as theirs. The only difference is it will be open and unencrypted.

The reality is if they want internet they will end up connecting to your rogue access point. Maybe they don't right away but most users are not that bright, impulsive, and impatient. Most "average" users get frustrated and go through the process even if they have doubts. The average user will connect to the network and even if they take the time to call their Internet Service Provider (ISP) their ISP will tell them their internet is working fine. Which it is. Seeing that it's their router that's the problem they will advise to contact their router manufacturer or connect to the new open network that has the same name to see if that works. Almost all of the time the tech will tell them to logon to the open network to troubleshoot the connection. I've experienced this professionally when dealing with companies/employees during a wireless network assessment.

The EvilTwin attack in the old days would require so many lines of syntax setting up the AP properly, trouble shooting, and all this shit but since people have modernized these attacks and created programs to automate the process we'll use an automated tool as well. This is the most effective way to obtain the Wi-Fi password after password cracking has failed you. The tool we'll be using is called **Wifiphisher**.

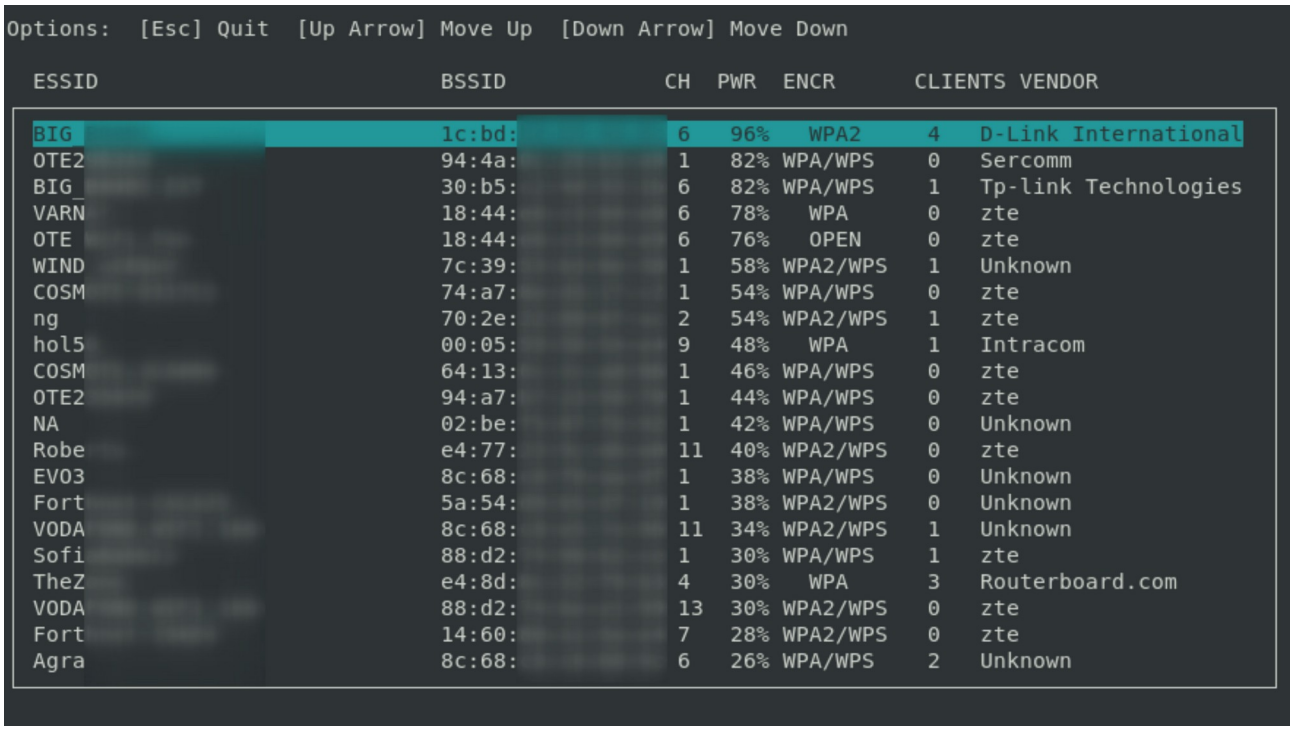
"Wifiphisher is a rogue Access Point framework for conducting red team engagements or Wi-Fi security testing. Using Wifiphisher, penetration testers can easily achieve a man-in-the-middle position against wireless clients by performing targeted Wi-Fi association attacks. Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients in order to capture credentials (e.g. from third party login pages or WPA/WPA2 Pre-Shared Keys) or infect the victim stations with malwares".

Make sure you have (2) wireless network cards (Alfa or otherwise) plugged into your Kali VM.
In Terminal in Kali:

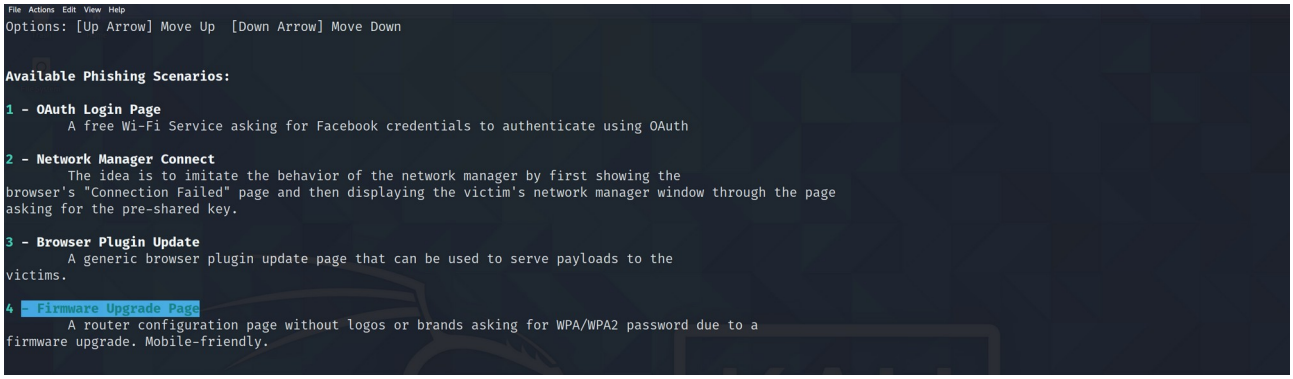
sudo airmon-ng check kill
sudo airmon-ng start INTERFACE
sudo wifiphisher

Let Wifiphisher scan the air for a couple of minutes to gain all the information possible. When you're ready select the Wi-Fi network you plan on targeting. It's best to target Wi-Fi networks with the best signal strength and that have clients connected to it to maximise all the attacks.

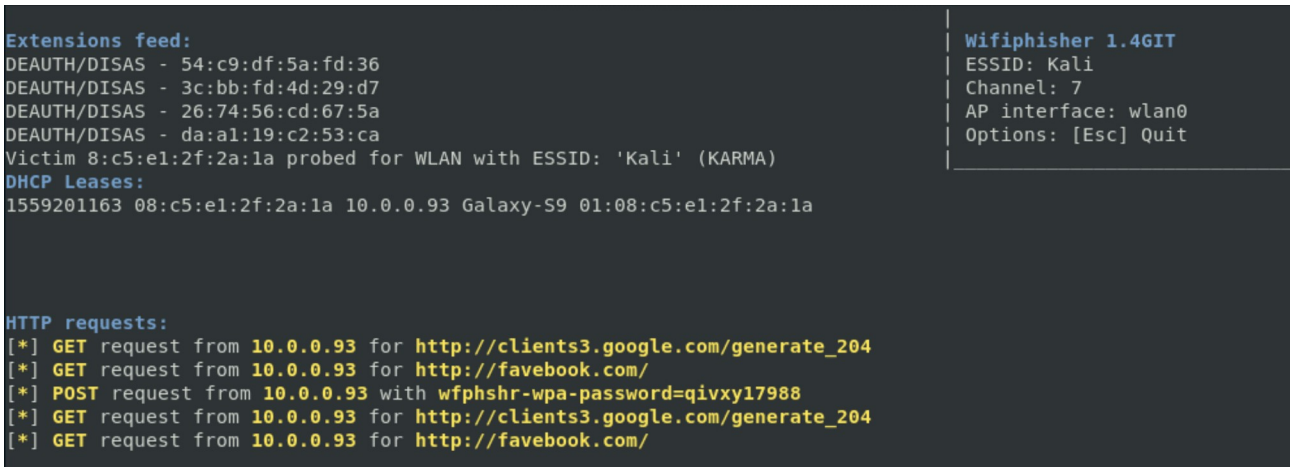
We target best signal strength for obvious reasons as these Wi-Fi networks are the closet to you. A good idea is to use your own laptops Wi-Fi card or iPhone/mobile device to see which have the best signal strength as these are the closet to you. The Alfa Wi-Fi cards might show a better signal strength for some networks when in fact your laptop Wi-Fi network card can't connect to them. The closer the Wi-Fi access point you're targeting is to you the better.



Once you've selected the targeted Wi-Fi network select "Firmware Upgrade Page".



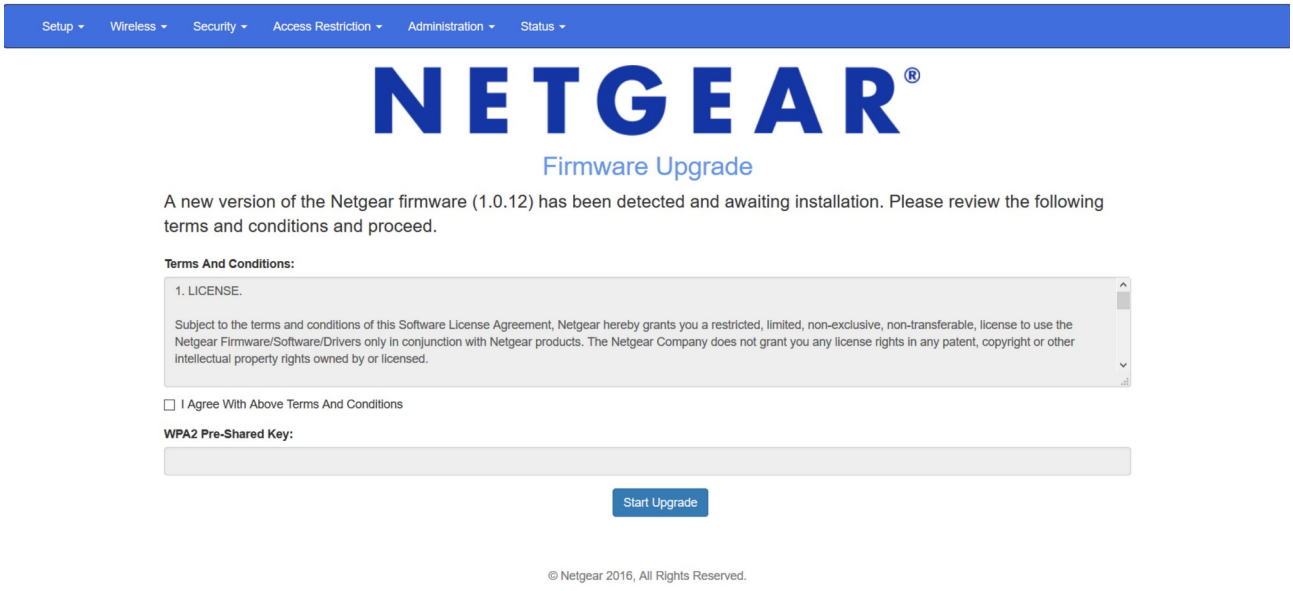
Next Wifiphisher will de-authenticate everyone connected to the targeted network.



Wait 1-3 minutes before checking the Wi-Fi network you've targeted to see if your attacks are working. After a few minutes you should notice the real Wi-Fi network is offline and you've cloned the Wi-Fi network name with an open Wi-Fi network for victims to connect. This is where we rely on the people that know the Wi-Fi password of the Wi-Fi network you're targeting to connect to the open Wi-Fi of their Wi-Fi network name and enter the Wi-Fi credentials.

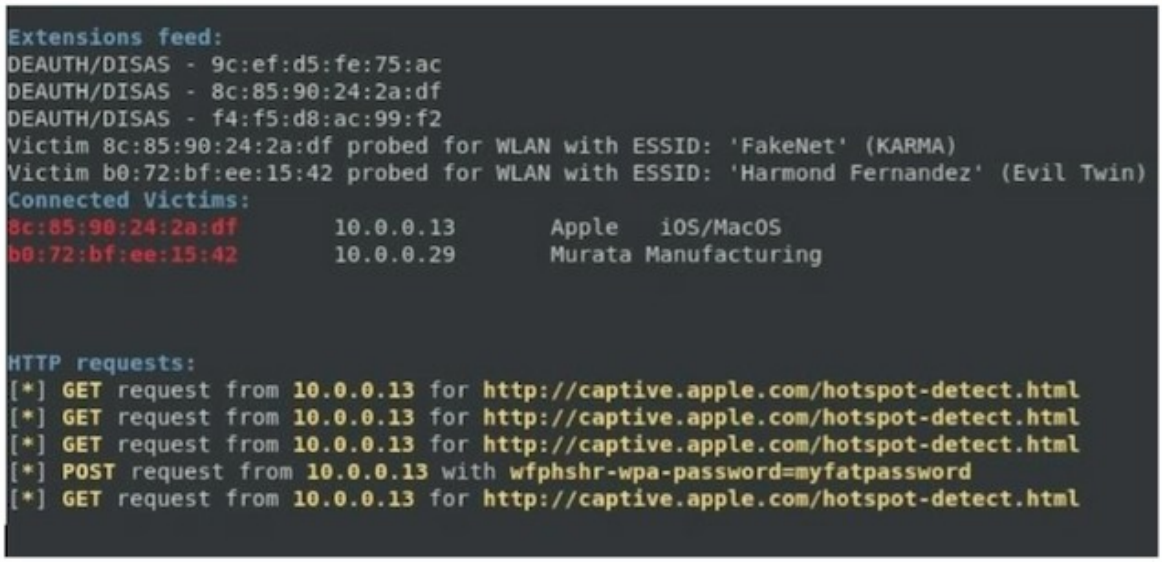
I suggest using this attack against your own Wi-Fi network to see exactly how your victim will be prompted with this attack.

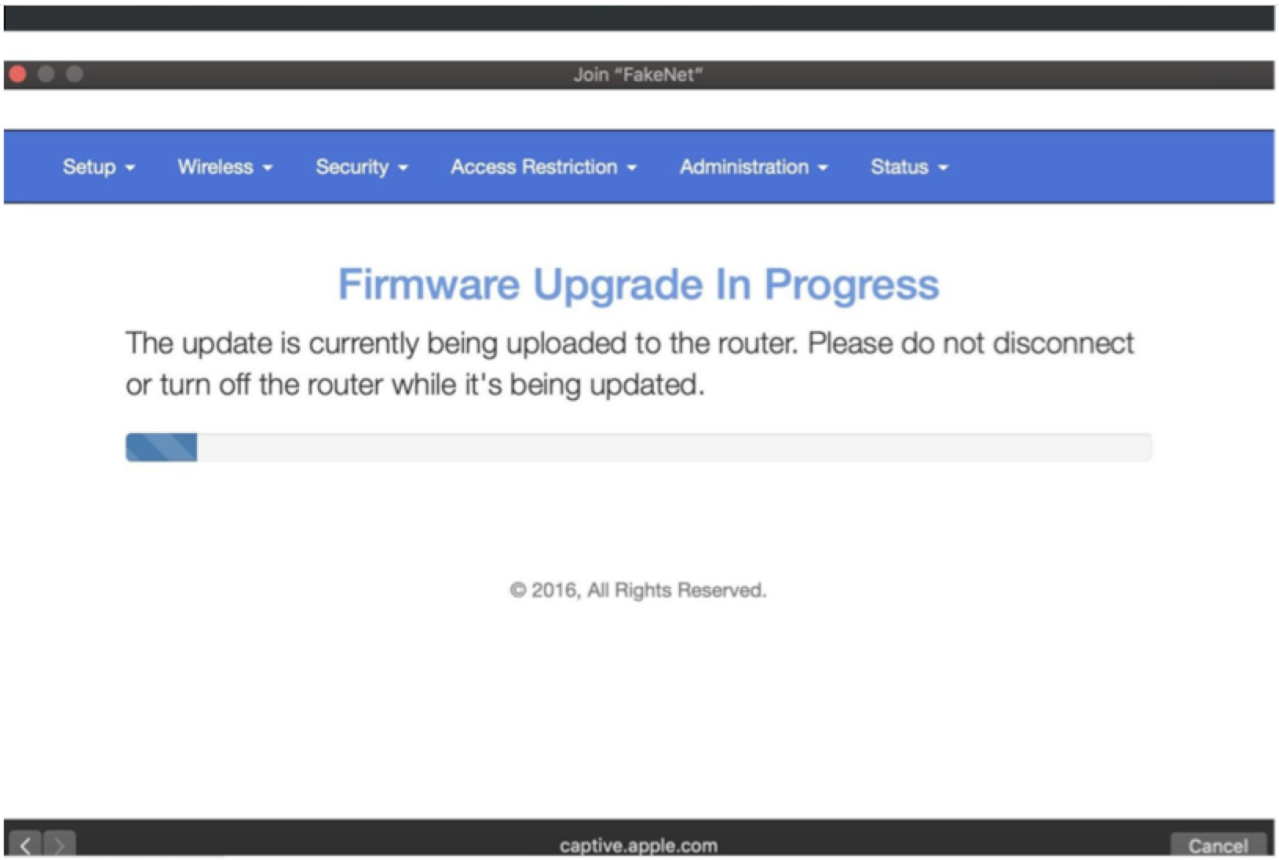
This is what is prompted to the people when they're tricked into connecting to your EvilTwin.



Once they've entered the Wi-Fi password it will be displayed in the terminal window where

Wifiphisher is running and the victims will be presented with an update screen. You'll want to take this attack down within 1-2 minutes after capturing the password if Wifiphisher doesn't automatically to avoid raising suspicion.





It's important to check your terminal screen that Wifiphisher is running in and to **PAY ATTENTION** to who connects to your rogue Wi-Fi network because you do not want to take down the target Wi-Fi network all day and have them call their ISP. You want them to connect, enter the credentials, and then you want to shut down your attack which will bring up their Wi-Fi network again. Wifiphisher is supposed to do this automatically but if it doesn't ensure you CTRL+Z it. Timing is key here not to raise suspicion but honestly this

depends on whom you're targeting. Don't launch your attack in the morning and then leave it running all day/night because that will be a problem, potentially.

Either way do what you think is best but understand by taking their Wi-Fi network down all day will draw unwanted attention. Maybe, maybe no.

Increase the POWER!
Another technique to increase your chances of success when hacking a Wi-Fi network is to increase the transmitting power of the Alfa network card to juice it the fuck up. When launching Wi-Fi network attacks it's best to be the closet and strongest signal to the target you're attacking. Depending on which Alfa network card you have this chapter may or may not be beneficial for you. Don't flip your shit if it's not as every card will respond differently.

Most Alfa network cards are capable of generating 1 WATT of power to increase the range of the Wi-Fi network card but by default are not setup to do so in Kali. We can tweak this shit by setting the transmitting power of the card to its max and boost our signal for best connection! Some people might have Alfa network cards that are capable of this and others do not depending on the one you purchased. If you get an error along the way, then you do not ;)

Update - The newest version of Kali creates issues with certain Alfa network cards that it worked on in the past. Some may have issues with increasing the power of the Alfa network card. Do not stress if this doesn't work as it's not the end of the world if it doesn't.

In Kali open up Terminal and type:
sudo iw reg set GY
`This command will set the region of your Kali machine to Guyana. Each country allows specific Wi-Fi regulations and by setting our OS host country to Guyana will allow us to increase the power beyond what is allowed in other countries. Certain countries don't want you to operate on certain channels whereas others do not have strict gudelines. By setting the country of our machine allows us to set different settings accordingly.`

sudo ifconfig
`Find your wireless card interface.`

sudo ifconfig INTERFACE down
sudo iwconfig INTERFACE
`Look for "Tx-Power=" and you'll see the default transmitting power. We want to increase this!`

sudo iwconfig INTERFACE txpower 30
`This will set the max power to 1W if your network is capable of this.`

sudo iwconfig INTERFACE
`Check again to see the difference with "Tx-Power=".`

sudo ifconfig INTERFACE up
`Bring the interface back up.`

Now that you've increased your transmitting power you'll be transmitting as the most powerful signal that card can put out. The downfall to increasing the transmitting power is you'll wear down your Alfa network card quicker than usual as it will generate more heat and energy. Personally, I found using it quite a bit after 2-3 years of owning one it would still function for my needs but not be as reliable as it once was (would disconnect randomly, drop connection, overheat, etc.).

Locating the Access Point (AP)

If you want to maximize this chapter you'll need to purchase another Wi-Fi antenna to fully benefit from this chapter. It's not %100 required but it will assist you moving forward and give you a better understanding of how you would be tracked when on a hacked Wi-Fi network. Some might implement this, and some may not.

The antenna we're wanting to purchase can be seen in the picture below and we'll need this type of directional antenna to help pin point the location of where the Wi-Fi network signal is coming from in order to increase the success of our Wi-Fi attacks.

You can purchase this type of antenna at:

https://shop.hak5.org/products/7dbi-panel-antenna
https://www.amazon.fr/Alfa-2-4HGz-RP-SMA-Screw-Antenna/dp/B003ZWPRUI
https://www.data-alliance.net/antenna-2-4ghz-7dbi-directional-panel-w-rp-sma-wif-signal-booster-fpv

Remember, it's ideal to be the most powerful signal around to maximize any type of Wi-Fi attack. We can accomplish this in a few ways.

The first way to achieve this is being as physically close as possible to the Wi-Fi network access point (AP) IE: your router.

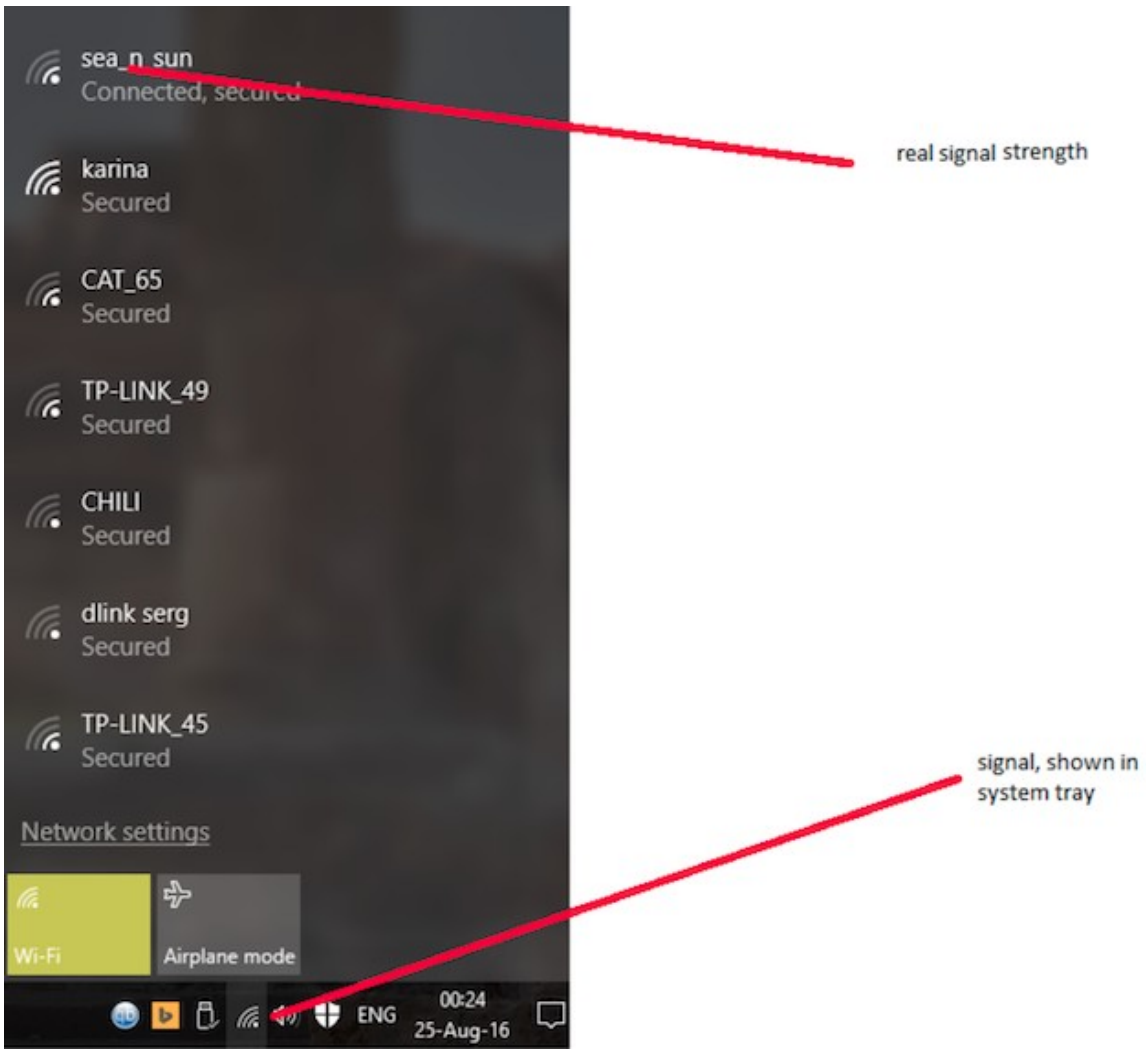
Obviously if you're sitting in the same room as the Wi-Fi router this would be ideal and best signal strength. Second method in achieving this is to increase the transmitting power of the network card itself. We can increase the signal transmitting power of the Alfa network card to make it a beast and be the most powerful signal around. We know that being as close to the target Wi-Fi router as possible is important when you plan on attacking it whether that's performing a DOS to bring the router offline or to be the strongest signal that others will connect to when launching an EvilTwin attack.

Let's talk about getting as close to the router as physically possible. This is pretty easy to do when it's your Wi-Fi router we're targeting right? So, get up and walk the fuck over to your router and then you can feel confident you'll as close as possible.

Obviously this isn't going to be possible for when you're targeting other people's Wi-Fi networks since you won't know where the router is physically located in their home/business which can make it difficult in determining if you're attacks are effective. I can guarantee there are times when you're trying to hack Wi-Fi networks and not having success because you're simply too far away to have any affect against the people you're targeting. Meaning, you're transmitting signal is too weak to make any meaningful attack viable.

There are times when it may appear that a Wi-Fi network near you is showing a strong signal strength when you're using Windows, macOS, or Linux but you're just not having success like you should when launching your attacks against it. You can't deauth the clients on the network and no one is connecting to your EvilTwin tricks.

I'm sure you've all had those times when you're targeting a specific Wi-Fi network but just can't get shit to work in your favor? You're launching an EvilTwin attack because you're unable to brute force the password needed to crack the WPA/WPA2 password or your attacks keep timing the fuck out? Not getting anyone to connect to your rogue AP nor getting a chance to capture their entered Wi-Fi credentials, right? Like what the fuck?! These attacks tend to be the most frustrating for new hackers because they don't succeed



every time, for multiple reasons, and most people don't understand why they're attacks are failing.

I know there are times when shit just doesn't work and you cannot check to see if it's even functioning properly depending on your skill level.

When you're new to hacking Wi-Fi networks it can be difficult to determine if:
A) Are your attacks not working on the specific target because they're not falling for your social engineering fuckery?
B) Are your attacks working properly from a technical standpoint?
C) Are you too far away from the Wi-Fi router?

We want to reduce the amount of failures and increase our chance of success for every attack we launch. Don't half ass shit when you're launching any type of attack and you'll succeed much more. Remember, be a professional and make your attacks as such. Treat hacking as a profession and act professional, you understand yes?

Remember, your host laptop Wi-Fi network card will display different Wi-Fi networks than your Alfa network card because they're different networks cards with different hardware specifications, obviously. Depending on how you want to connect to the internet you want to make sure the host Wi-Fi card is displaying the best signal more so than the Alfa. Alfa

networks can be used, of course, to connect to Wi-Fi networks but depending on your setup you might prefer your host computer to be connected to Wi-Fi network and then launch Whonix VM or use the Alfa network card in Tails to connect to a Wi-Fi network far away.

Lastly, you can install the Alfa network card drivers on your host OS and use that too for main Wi-Fi connection or just hooked to a VM. Plenty of options depending on your setup and comfort.

Let's look at an example:
You're sitting at coffee shop and have a Wi-Fi network you want to hack but is the access point (AP) across the street or (4) floors above you?! What barriers does that Wi-Fi signal have to go through before getting to you? Are you the closet and strongest signal so that when you launch EvilTwin attacks the Wi-Fi owners connect to you or what? Will the connection be stable enough to even connect to from your location? Many things to know.

Maybe you want to "work" from your home comfortably, so you decide to compromise every Wi-Fi network around you which is what most people end up doing. This way you're stationary but have the comfort of knowing you're not using your own Wi-Fi network. This isn't recommended but sometimes you just don't want to leave the hotel or your bed so you aim your directional antenna down the street and compromise a Wi-Fi network 100m from you. ;)

Me personally, I will literally compromise as many Wi-Fi networks as possible wherever I am and rotate them accordingly to help evade any chance of tracking me because I always assume the worst. Damn that paranoia! Compromise the whole apartment building across the street and jump from Wi-Fi network to Wi-Fi network on the daily if need be! Figure out what risk is acceptable to you and get to it!

Here's another example.
You live on 5th floor of 10 story apartment building. Now picture every floor is just one unit. So, you live on 5th floor and no one else but you lives on that floor as does your neighbor who lives above you who lives on one floor and so on. Based on this hypothetical example this means only 10 people will live in your building since it's a 10-story building you understand? Picture you're sitting in your living room which is on the North East side of the building and the Wi-Fi network you're attacking is one floor above you but on the South West side of the building. The Wi-Fi router you're targeting is the farthest from you but still reasonably close that you should be able to see it available when looking for a network to connect to. Depending on how far this signal is will dictate the best chance of your Wi-Fi attacks and maintaining a connection to it.

I remember back in the day I would be launching a DoS attack against a Wi-Fi router in order to bring the router down so I can launch an EvilTwin attack but couldn't get the router down. I didn't realize at the time I was too far from the router with multiple physical barriers that can fuck up the Wi-Fi signal between me and the AP which was contributing to my failures. You might be walking around with your laptop looking for the best signal

and find one but what you don't realize is that Wi-Fi signal is bouncing off walls and other things giving you a false sense of the Wi-Fi signal strength. This will make your connection to the network terrible along with the chances of successfully hacking it decreased.

It would be better if you knew exactly where the AP was physically located and then move towards the signal so you can maximize your attacks and have the best Wi-Fi signal strength possible. Remember, you want to be as close to the AP as possible and be the strongest Wi-Fi signal that your target(s) only see your rogue AP in order to maximize an EviTwin attack and other Wi-Fi network attacks.

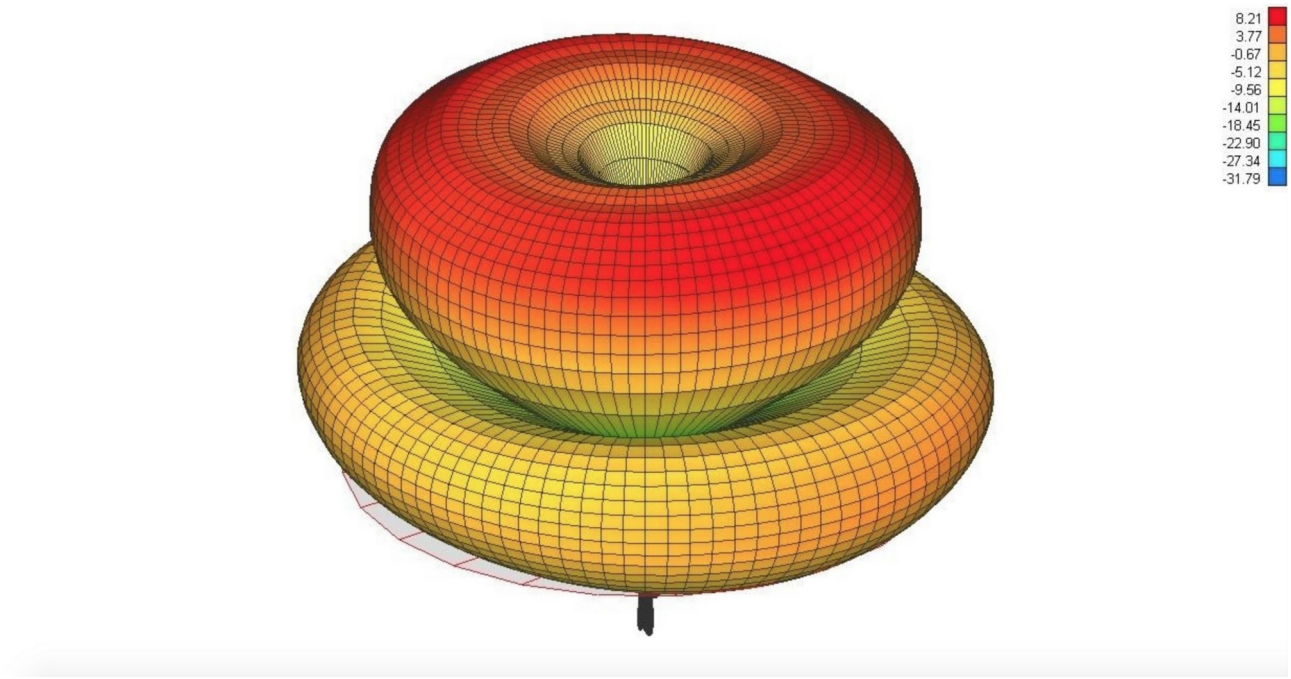
This actually took me some time to figure out how important this was when I was first starting out with Wi-Fi hacking and it wasn't until I was hired as a professional cyber security consultant that I learned the importance of this and the techniques needed to maximize the chance of success with my Wi-Fi attacks.

OK now we're going to focus on your own Wi-Fi router to determine roughly where it is in relation to your physical location so you understand how to use this technique against other W-Fi networks. Once we know where the Wi-Fi router is physically located, we can then "aim" our antennas towards the AP in order to increase our chance of compromising the Wi-Fi network.

In Chapter 2 we briefly talked about different antennas and how you should upgrade when you feel the need to do so. When you purchased the Alfa network card it would've came with a small omnidirectional antenna that can be replaced with different antennas. The antenna that comes with the card is an omnidirectional antenna which are good when you don't know where the Wi-Fi signal is coming from and are ideal for trying to connect to Wi-Fi networks that are on the same floor/level as you.

In the screenshot below is a typical omnidirectional antenna that you should be familiar with.

Below is a picture of the potential range of coverage an omnidirectional antenna can cover.



As you can see omnidirectional antennas are ideal for connecting to a wireless access point on the same floor but aren't suitable for connecting to any network outside its range. It's like a donut range, right? An omnidirectional antenna range can capture, intercept, and broadcast signals within that donut shape and the farther they are away from the antenna the weaker the signal is. Easy to remember!

As discussed previously about omnidirectional antennas it's best to think about the range of an omnidirectional antenna as the light that comes off of a lamp with a lampshade on a night side table. Picture when you turn on the lamp and the light that it gives off is that of how an omnidirectional antenna range looks like. As far as that light may reach would be the range of the omnidirectional antenna. Whereas directional antennas are more like the light that comes from a flashlight. Like a laser pointer type of beam for a signal you understand?

Omnidirectional antennas make it difficult in determining where the Wi-Fi network signal is coming from since the signal is equal from every direction whereas directional antennas can help you focus on one direction and therefor assist in determining which direction the Wi-Fi network signal is coming from. Like a flashlight shining some light into the dark! :)

Remember, directional antennas are like a laser pointer when looking for the Wi-Fi network signal whereas omnidirectional antennas are like the light coming from a lamp. Hopefully this makes sense and can help with your learning.

Using the right software along with a directional antenna sweeping through the air will result in the signal strength getting stronger when then antenna is pointed in the direction of the AP and weaker when the directional antenna is pointed away from the signal. Obviously. If we're aiming our antennas towards the signal the signal strength will increase

so this would make sense and we can use this to determine where exactly the Wi-Fi signal originates.

We utilize this feature in order to hunt down the access point and focus our efforts in compromising it. The same techniques are used to catch hackers and rogue devices connected to a network. If you've ever wondered how an attacker is physically located when connected to a hacked Wi-Fi network this is a technique used to locate you. Just because you're on a hacked Wi-Fi network doesn't mean you still cannot be located, don't be naive. Since we can locate the AP based on signal strength law enforcement would be able to locate your location when connected to a Wi-Fi network based on your signal strength if they're in the area hunting for you! This is why it's important, like I talked about before, to hack as many Wi-Fi networks as you can that way you have many Wi-Fi networks available at your disposal to be more difficult to catch. Move around frequently if possible.

Should there be a mistake on your part and law enforcement is looking for you since you use so many different Wi-Fi networks it would be much harder to track you and would take a lot of manpower and finances to do so. Hack as many Wi-Fi networks as possible and rotate them monthly, weekly, or daily depending on your paranoia level.

Using the newly purchased directional antenna in this chapter and Wireshark we can create a display filter to target a specific AP signal and plot it on a graph in real time. This way when you're using the directional antenna you're literally sweeping it around the area/location like a metal detector in the air looking at the signal strength graph to determine the AP exact location.

If you've never used Wireshark before and you're not familiar with it you can check out some very useful YouTube videos or purchase Wireshark books online from amazon or eBay. There are plenty of tutorials surrounding Wireshark and I won't go into details about the program because that's a book on its own.

Book recommended for learning Wireshark

There are other tools people use to track down a rogue AP or Wi-Fi network but I've always used Wireshark and I think it's a good tool to learn so let's stick with it. It's very easy to use so don't get overwhelmed! Once you see how easy it is and how important it is to properly track down the Wi-Fi network you plan on targeting you'll be using this technique all the time for your Wi-Fi hacking madness.

At the end of this chapter you'll find a link to a video which will help solidify this new knowledge. Please read first and try to follow along and then watch the video to help with visuals if needed.

It should be noted that I copied this exact technique from Kody at nullbyte so props to him for explaining it all. I always found it difficult to explain it to others as I used a proprietary program stolen from a previous employer so support Kody if you can because this is his work.

The only thing you need to do first is determine what channel your target Wi-Fi network is on. It's important to put your Wi-Fi network into monitor mode first and then scan for Wi-Fi networks around you. If you followed the YouTube videos on the Wi-Fi megaprimer with Vivek you should be familiar with aircrack-ng and how to put your card into monitor mode. If not, this is OK as we'll talk about it now.

When you're following along below it's best to target your own Wi-Fi network/router so you have a much better understanding of how to properly find another AP with the strength of the Wi-Fi network signal.

We need to put the Alfa network card into monitor mode and then select which channel to sniff the wireless traffic on manually because Wireshark cannot control the wireless card by itself, so we need to do this first so Wireshark is all setup properly. Let's get into it.

For this example, I'll be using "wlan1" as my interface but yours could be different.

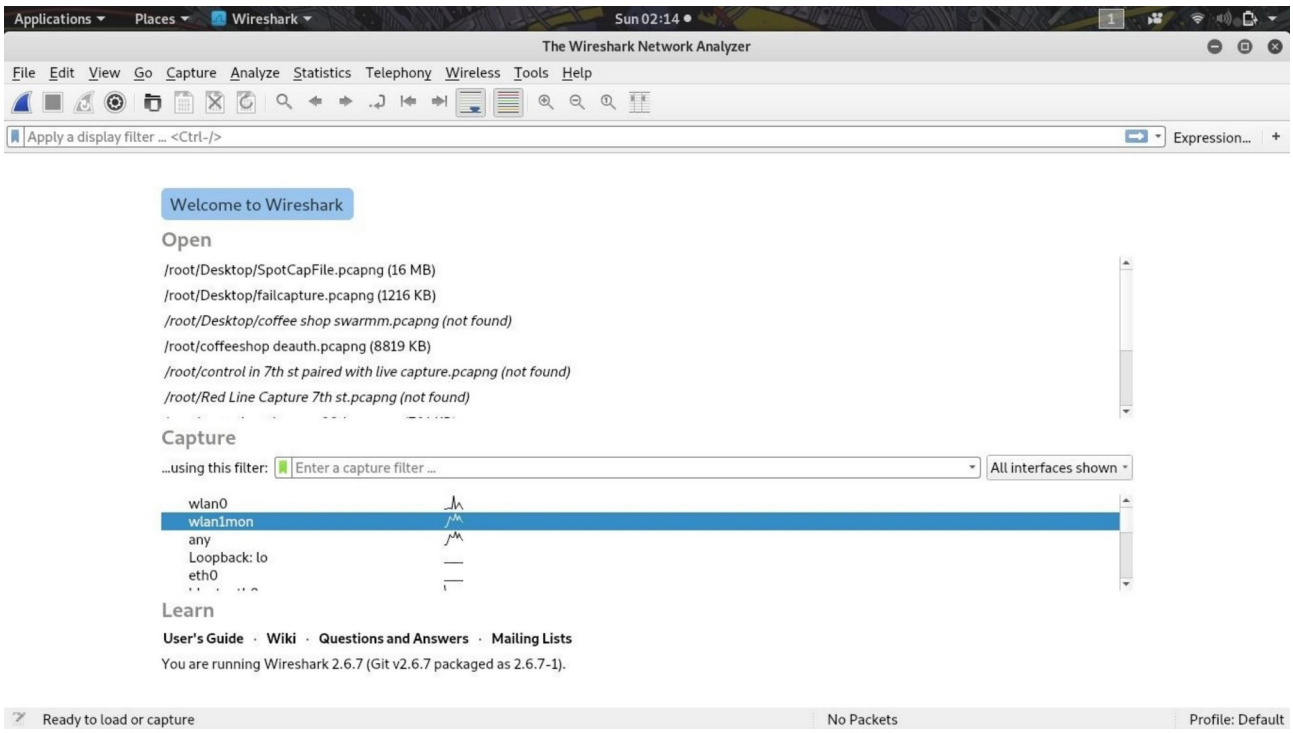
In Kali type the following:
sudo airmon-ng check kill
sudo airmon-ng start INTERFACE
sudo airodump-ng INTERFACE

My example:
```
sudo airmon-ng check kill
sudo airmon-ng start wlan1
sudo airodump-ng wlan1mon
```

Locate your Wi-Fi network and take note of the channel it's on. Once you know the channel cancel airodump-ng with **CTRL+C** on your keyboard and then type:
sudo airodump-ng INTERFACE -c CHANNEL

My example:
```
sudo airodump-ng wlan1mon -c 1
```

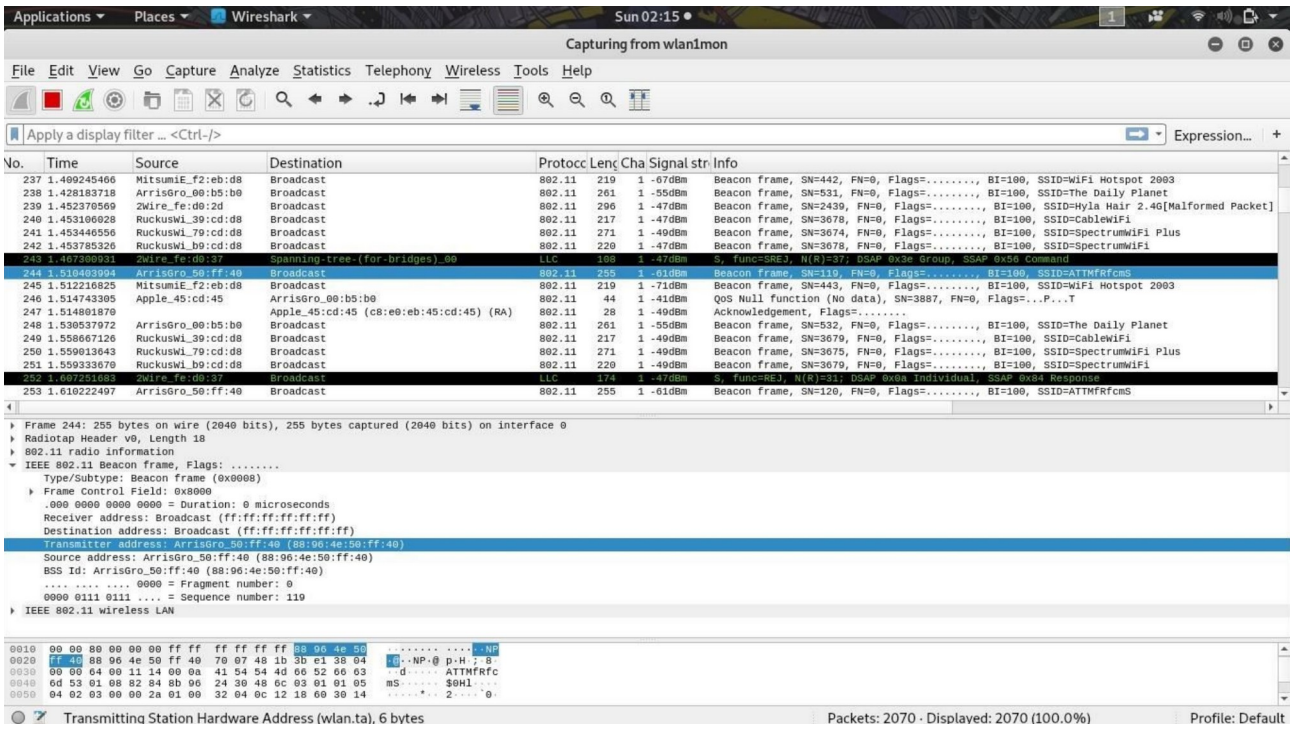
We now have our Alfa network card in monitor mode sniffing Wi-Fi network traffic on channel 1 and we're ready to launch Wireshark. Open Terminal and typing the following:
sudo wireshark &



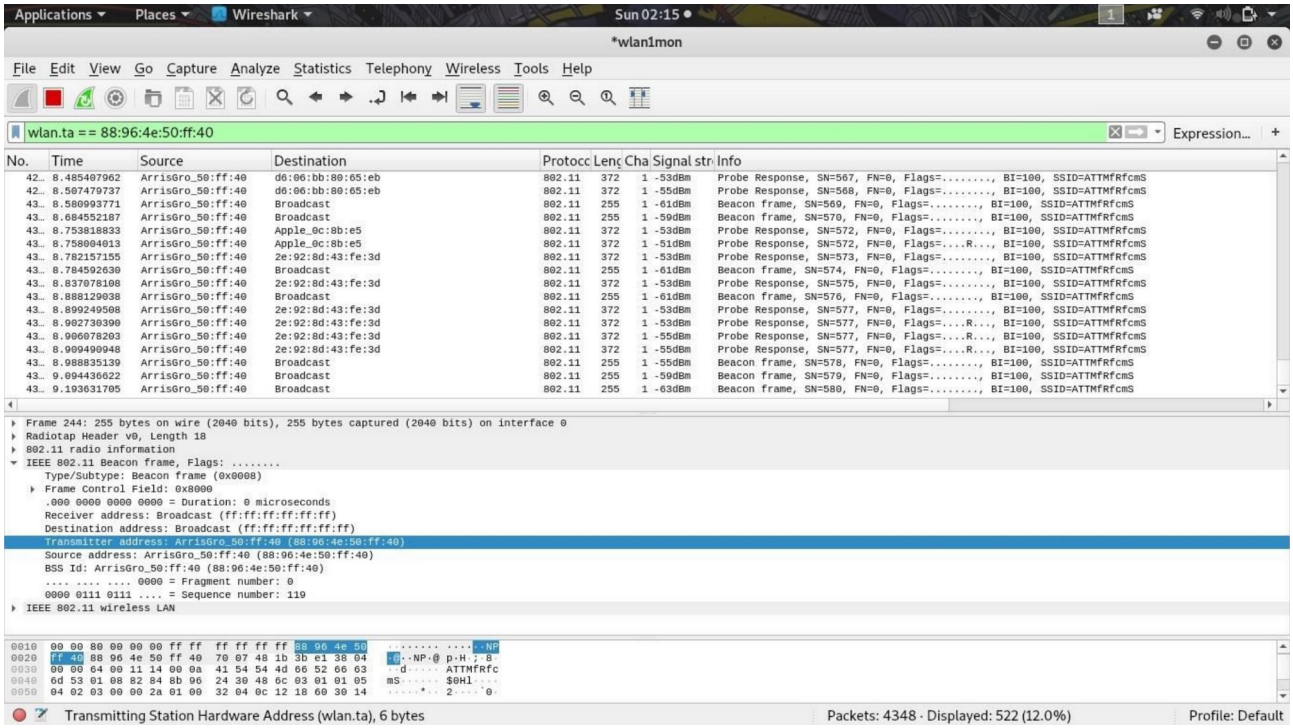
Once Wireshark is loaded select your monitor interface to capture the data packets on that interface. My example monitor interface is "wlan1mon" as seen in the screenshot above.

Once you've selected your monitor network interface, you'll see a bunch of data go by the screen in WireShark. Wait about 20 seconds and then stop the capture by clicking on the STOP button in red located on the toolbar on the left-hand side.

Locate your own Wi-Fi network by scrolling through the data captured by Wireshark. You should be able to see your SSID of your Wi-Fi network (the name of your Wi-Fi network). Left click on it to highlight it then click on the arrow next to "IEEE 802.11" and look for the "Transmitter address" or "Source address" field. That's what we'll use to build our capture filter to show only the device we're hunting for. You can see in the screenshot below I've left clicked on my Wi-Fi network and then clicked on the "IEEE 802.11" tab and have highlighted "Transmitter address".



Right click on the "Transmitter address" to show a list of options then select "Apply as filter" and then "Selected" in order to create a display filter that will only show packets transmitted from that specific device. This filter will show all Wi-Fi transmissions from that target network and nothing from unrelated networks.



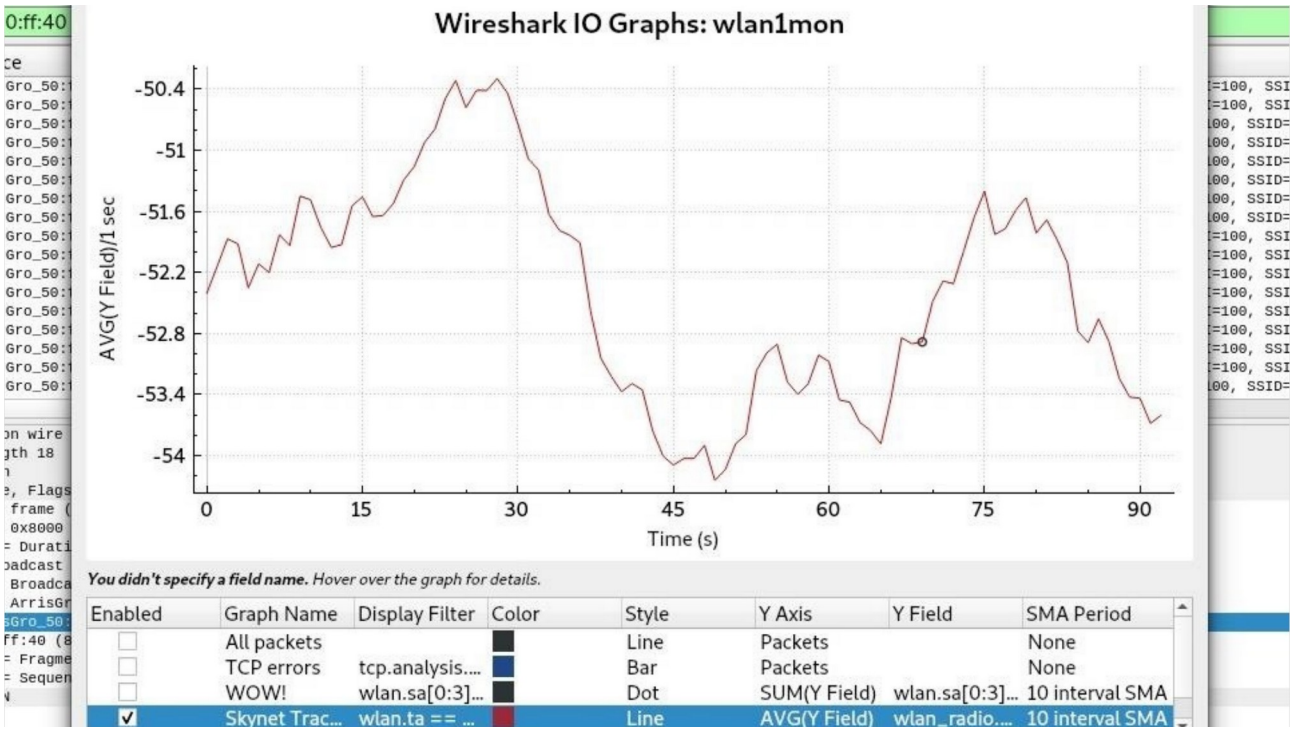
You should notice a new filter in the filter bar that looks like "wlan.ta ==". Copy that whole display filter as we'll need it for later. This is important!

To re-cap:
We've isolated the Wi-Fi network we're targeting by first determining what channel it was on and then we created a filter in WireShark to show the packets only from the device we want to attack. Once we've isolated the Wi-Fi network signal we can then switch to visualizing the signal strength which will help us locate the AP. Again, I want you to picture the motion when someone is using a metal detector on the beach but instead is waving an antenna in the air looking for the power strength of the Wi-Fi signal! Same type of concept and motion.

Remember,' there's a video at the end of this chapter to help walk you through it all should you get confused with the directions so don't stress if you're confused because the video will help.

To start the visual graph for the signal strength, copy the display filter we already created with WireShark (told you it was important) and click on "Statistics" and then then "I/O Graph" to launch the WireShark visual signal window. Once that's loaded click on the plus (+) icon to create a new graph and make sure you uncheck any other graphs that may be enabled.

You can name your graph whatever you like. Remember the WireShark display filter you copied before? Paste that into the Display Filter field beside your graph name. For the "Y Axis" column select "AVG(Y Field)". For the "Y Field" column paste "wlan_radio.signal_dbm" into it. Finally, set the SMA Period to "10 Interval SMA". Once you've finished that shit your settings should be similar to the screenshot below and your signal strength graph should begin.



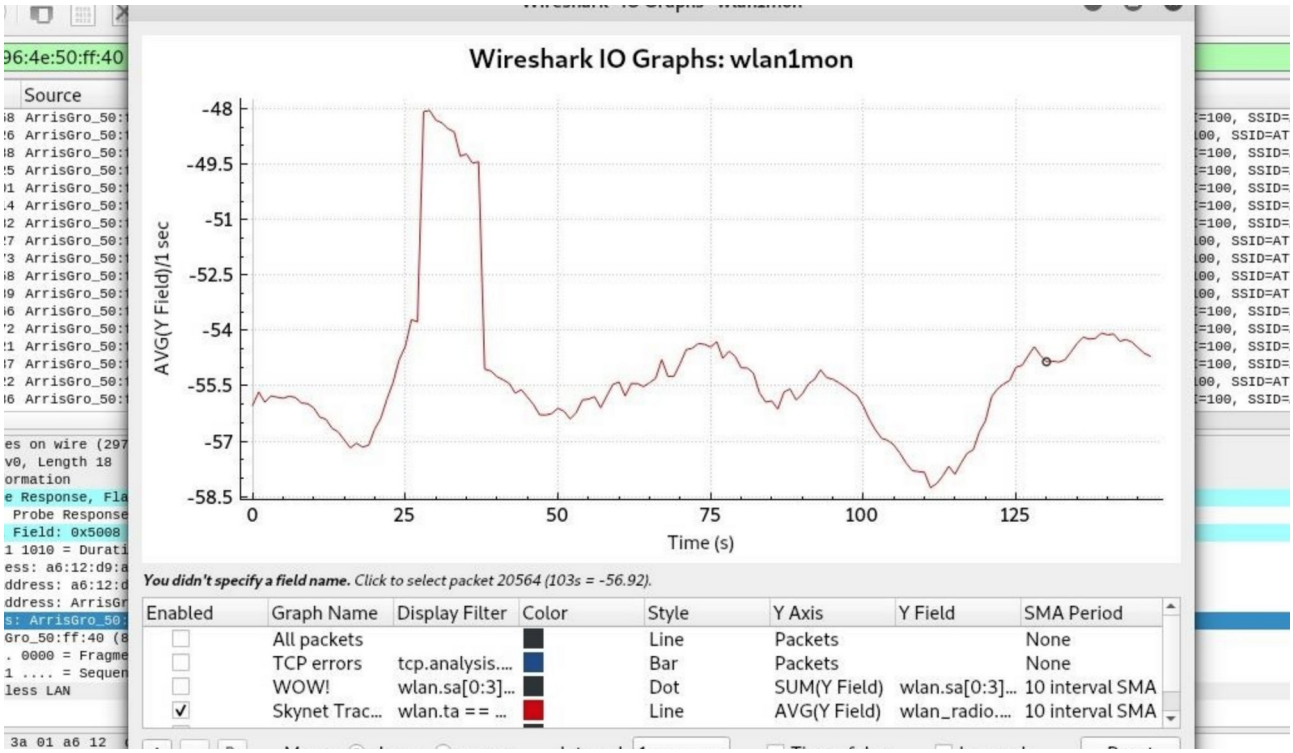
Ok now exit out of the I/O graph and stop the Wireshark capture. Place the Alfa network

card antenna away from your AP (preferably face down on the floor) and then restart the WireShark capture. Once you've restarted the WireShark capture select "Statistics" and then then "I/O Graph" to launch the WireShark visual signal window again. Now we have a fresh graph and a baseline to work with.

Leave your Alfa network card with the directional antenna faced down on the floor for (10) seconds to let it gather data for a base line reading. This graph will show you the average signal strength from your targeted Wi-Fi network over time. The signal may seem to fluctuate a lot at first because Wireshark is graphing the small changes in the signal. Signals can bounce the fuck all over the place as well so it may appear a little chaotic at first. The graph will all make sense once you pick up the directional antenna to sweep through the air visually seeing a stronger and weaker signal represented on the graph.

OK once you've left the Alfa card face down for (10) seconds pick it with the directional antenna and slowly sweep it around your place and watch the graph. I recommend to start facing away from your own AP and then slowly rotating towards it while watching for a spike on the graph to indicate which direction the Wi-Fi signal is coming from! Keep rotating it around until it's pointing towards your AP. You should be able to detect a spike in signal and begin to locate the location of the AP. Once you have a spike on the graph keep it steady and walk towards the signal and do another sweep to begin really narrowing the AP location down! See how the graph changes?! Try this from various distances to see how this works and feel comfortable with this technique.

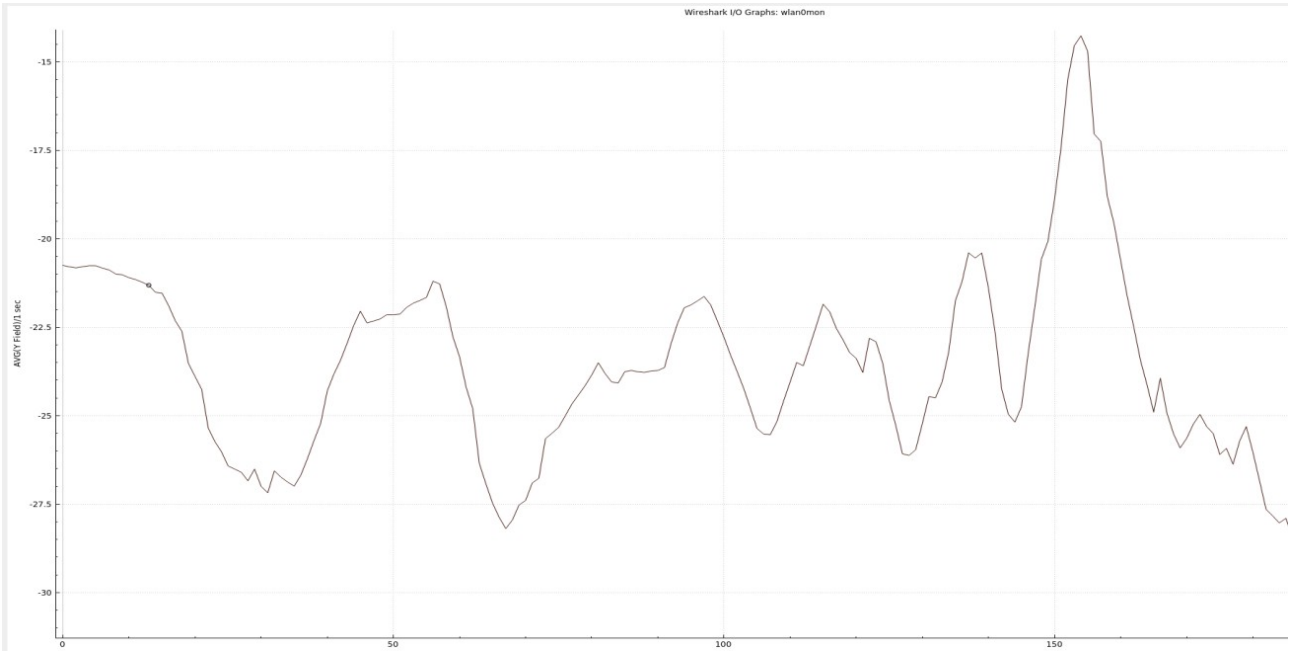
In the screenshot below you can see a spike in the signal strength indicating the directional of the Wi-Fi network access point (AP).



That spike is the strongest signal in that particular direction. Obviously when targeting

your own Wi-Fi network' you can physically walk towards the location of the AP with the antenna to test signal strength. This would be no different when targeting any other Wi-Fi network.

Below is a screenshot of my AP I was targeting.



Notice the power levels on the left-hand side in the screenshot above?
-20
-22.5
-25

This is the power level that I had when I was 10FT away with my antenna pointed at my AP. If you're targeting an AP with a power level of -65 or higher, you're too far from it to launch any meaningful attack on it. Keep your AP targets ideally within 0 to -55 ranges. If you have a weak signal walk towards the direction of the spike and see if you can close the gap.

You'll also notice in the screenshot above the graph is fairly chaotic with a lot of spikes here and there but you can tell there is difference in one of the spikes yes? Sometimes your baseline will be all over the place and it can be difficult to determine what is what. Take your time and swivel the antenna around until you can see that obvious spike from the others and focus in that direction. Like anything you need to practice and the more you practice the more comfortable you'll be with it all which means the more effective you are at launching your attacks.

This skill and technique are important when locating the direction of the Wi-Fi network you plan on targeting. For me, there are times when I prefer to work outdoors and sit down on a park bench so I have my long-range directional antenna hidden inside my backpack aimed towards a specific building to hack onto a Wi-Fi network and use it for the day. I use

this technique every time to determine exactly where to try and aim my long-range antenna to maximize my attacks and connectivity to the network. You should incorporate this into your hacker toolbox as well :)

This technique is better explained by the video below if you have issues.

Click to watch Video

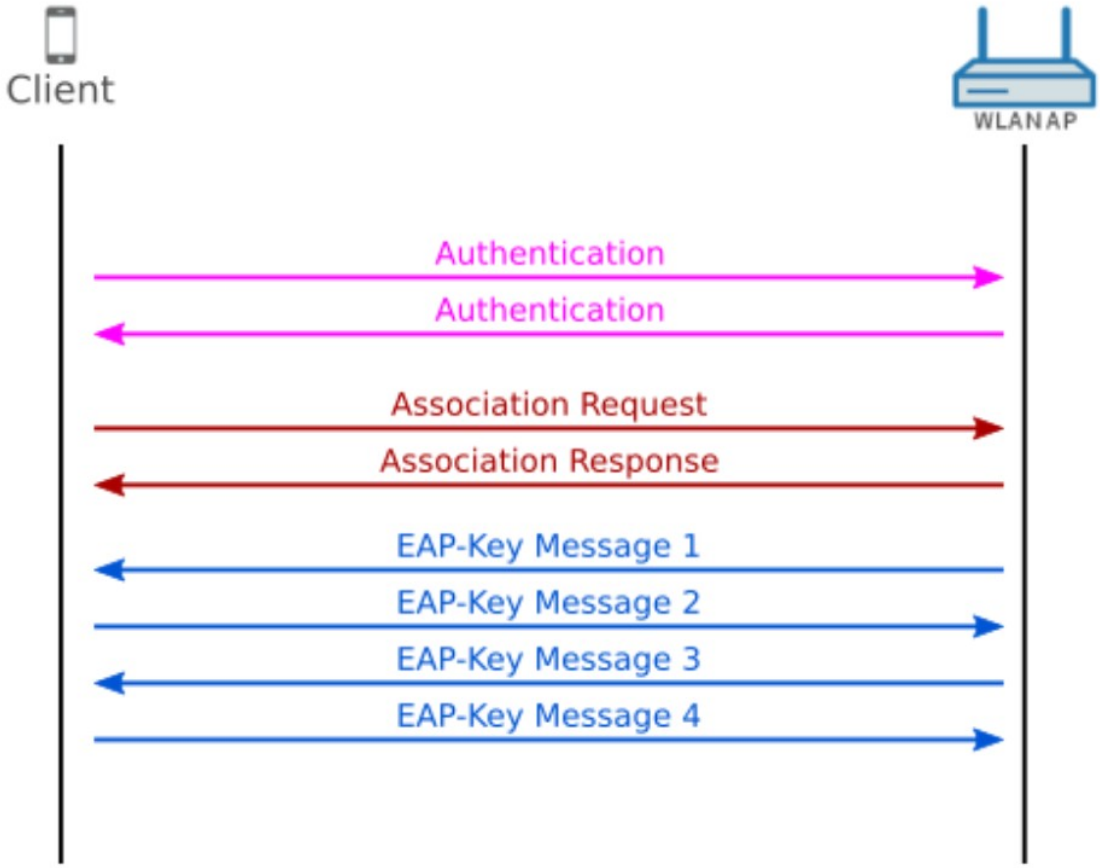
WPA3 Networks

Since WEP, WPA and WPA2 protocols have their own type of vulnerabilities that attackers like us abuse the fuck out of, the industry has tried to better secure wireless networks by implementing a new standard called WPA3.

WPA3 was created and introduced in 2019 but for me personally I haven't really encountered too many networks secured with WPA3 but this chapter is meant to get you up to date.

WPA3 only uses "Advanced Encryption Standard" (AES) and no longer uses older protocols like the "Temporal Key Integrity Protocol" (TKIP) or "Wired Equivalent Privacy" (WEP) seen in previous WPA/WPA2 protocols.

The screenshot below is a quick refresher on how WPA/WPA2 protocols secure wireless communications.



If you can recall WPA/WPA2 protocols rely on the Pre-shared Key (PSK) as its main authentication for connecting to a Wi-Fi network. The WPA3 protocol uses a different method of authentication called Simultaneous Authentication of Equals (SAE). If you can recall when cracking the WPA/WPA2 Wi-Fi network password we do this by capturing the 4-way handshake and using a massive dictionary wordlist to brute force the password yes?

We can do this all offline and on our own time. Hopefully this rings a bell. WPA3 makes this no longer possible because as soon as the AP notices too many SAE requests it will use tokens in order to limit the number of attempts. Eventually you'll be limited in the number of guesses at the password so cracking the password online isn't going to be a realistic option unless you plan on living forever.

As the password/passphrase is no longer part of the PMK, the complexity of it no longer plays an important role. Therefore, it is suitable to use passwords that are easy to enter and remember. However, you should still go for a complex enough password, so that an attacker is unable to guess your passphrase within a short amount of time. Although offline dictionary attacks are prevented, the access to your network with a guessed passphrase is still possible.

So, we now know that cracking the password from a WPA3 enabled network is not reality. What about EvilTwin attacks?

WPA3 enabled devices use Protective Management Frames (PMF) which protect against attackers being able to forge management frames. If you're confused on what management frames are please re-watch the Wi-Fi megaprimer YouTube videos in Chapter 4 delivered by Vivek as he does a much better job at explaining this. It's a good idea to re-watch those videos as a refresher from time to time so dive in bros!

PMF protects against when an attacker disassociates a user from the network and making it seem they're the Access Point (AP) that the client was currently connected to. If you're confused on what the fuck this means it basically means no more EvilTwin attacks against WPA3 only devices. You can't disassociate someone connected to a WPA3 network thus you cannot trick them into connecting to your rogue access point. Shit isn't happening.

One of the main advantages of WPA3 is the underlying Dragonfly handshake which replaced the 4-way handshake that was used in WPA/WPA2 networks. This Dragonfly handshake was supposed to make it impossible to crack the password, but security researchers found that hackers can still recover the password of a WPA3 protected Wi-Fi network with some hacker fuckery.

The (2) flaws surrounding WPA3 are downgrade attacks and side-channel leaks which can be abused to recover the password used by the Wi-Fi network known as CVE-2019-13377 and CVE-2019-13456.

https://github.com/vanhoefm/dragonslayer
https://github.com/vanhoefm/dragondrain-and-time

Conclusion

You should be familiar, if not very comfortable, with what has been discussed in this course. Remember hacking does not happen overnight so it's best to constantly practice to become more efficient and effective.

Every place you setup shop try taking over as many Wi-Fi networks in the area as you can. We know that you can target "all" networks using wifite and let it run automatically in the background for you. There's no reason you can't do this while sipping your coffee at the same time. The more WiFi networks you're able to use the better it will be for you. Nothing better than sitting at a coffee shop using the WiFi across the street to launch your attacks. Use a different network every time you can and move around if possible. Before you know it you'll have 30+ Wifi networks to use. This will increase the chance of remaining anonymous and reducing the risk of being caught or tracked to one location should something occur.

You should be able to be a ghost online using other Wi-Fi networks with your OPSec on point by now if you've been following along in order with the courses at HackTown. You should know how to hide your tracks and prevent from being indeitified while launching a cyber attack, posting online somewhere, checking your vendor account, hacking the planet, or doing anything that's questionable online.

Building on this knowledge the next course at HackTown being ACT II consists of what to do once you've hacked onto a Wi-Fi network and how to target the individual(s) on the network for profit and pirating. This includes up to date Man-In-The-Middle (MITM) attacks, malware delivery, and sniffing for passwords on the network.

The hacker maniacs who are reading this wanting more knowledge I suggest researching "Ethical hacking", "penetration tester", and "pen tester". I don't know your hacking knowledge level but for those who are like WHATTTTTT THE FUCK IS THAT these are the search terms that will allow you to follow up on the "professional" careers in hacking. The point is to educate yourself on how professional hackers operate against certain websites/organizations that have hired them to hack their company so you can begin to adopt their methodologies for your own goals of taking over the world. You can download the "Certified Ethical Hacking course" from any torrenting website and read at your leisure along side these courses at HackTown to dive deep. It's highly recommended to do as it will help your knowledge base moving forward to cyber criminal master.

Stay focused when learning everything here if this is all new to you and make sure your comfortable with everything before moving forward. Like any University, college, or any other acedemia shit doesn't happen over night and realistically expect this to be just a long. Don' get lost down the rabbit hole.

I hope you enjoyed Act I and can now compromise Wi-Fi networks around you and use them for your devious polans.. Until next time comrades.