JOHN SMITH

WI-FI HACKING

WIRELESS HACKING FOR BEGINNERS - STEP BY STEP

Wi-Fi Hacking

Wireless Hacking for Beginners - Step By Step

John Smith

Introduction

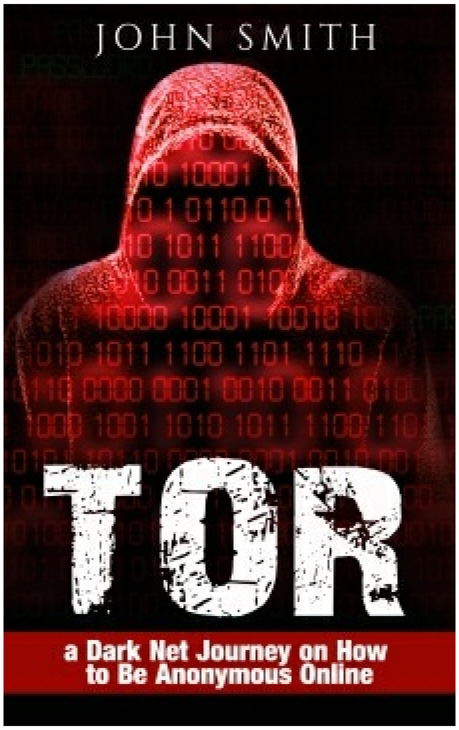
Hacking, hackers, cracking… these words are often thought of as bad, negative or worse, evil. And you can't blame people for thinking so. After all, getting into computers and computer systems by trying to get around installed security features and programs isn't something that people take kindly or positively. It can be compared with knowing that someone is trying to break into your home in the middle of the night and feeling scared or angry at the audacity of such actions.

But believe it or not, hacking isn't all bad or evil. You may even say that to some extent, hacking is a necessary evil and such necessary hacking may be considered acceptable or even ethical. The difference being is that unethical hacking on other people's Wi-Fi networks for purposes of personal gain or harming others is unacceptable and is not the purpose for this book. If you're reading this for personal gain or revenge, I'm sorry, but you're reading the wrong book, though the methods presented here apply to both ethical and unethical hacking.

In this book, you'll learn what constitutes ethical hacking, apart from the fact that it's meant to help others, how to hack the 2 types of Wi-Fi networks easily and some of the most common hacking-related terminologies, especially if you decide to study more advanced hacking techniques later on.
So if you're ready to get hackin', in a good way of course, then turn the page and let's begin.

Table of Contents

URL: http://amzn.to/2juBmFS



Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

Legal Notice:

Disclaimer Notice:

Please note the information contained within this document is for educational and entertainment purposes only. Every attempt has been made to provide accurate, up to date and reliable, complete information. No warranties of any kind are expressed or implied. The author holds no liability should the reader engage in illegal activities. Readers should acknowledge that the author is not engaging in the rendering of legal, financial, medical or professional advice. The content of this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, which are incurred as a result of the use of information contained within this document, including, but not limited to errors, omissions, or inaccuracies.

Chapter 1: Wi-Fi 101

Before you get to learn how to hack Wi-Fi systems, you’ll first need to know what it is! You can’t hack something you don’t know, right? So before we go any further, I’ll expose you to the basics of Wi-Fi.

Basically, Wi-Fi is the shorthand version of the term Wireless Fidelity. It’s a high-speed network and Internet connection that doesn’t need cables, wires and countless other things that can clutter up a space or worse, cause you to fall flat on your face due to tripping on such things. If you look at it, Wi-Fi is much cheaper and easier to put up and manage compared to wired networks. Primarily, this is because you don’t have that many wires to work with and trip over on. Also, being wireless in nature allows you to move your equipment – routers and computers – around the place easily and quickly because you don’t need to burden yourself with looking for ways to position the wires and cables so you and others won’t trip over them as well as looking for places with phone sockets. And best of all, Wi-Fi networks allow you to connect multiple devices of different technologies from desktop computers, laptops, and smart gadgets such as phones and tablets. In fact, you can only connect to the network with smart-phones and tablets via Wi-Fi – cabled networks aren’t an option. Outside your personal working or home space, Wi-Fi is becoming more and more accessible in public spaces too, such spaces being referred to as “hotspots”.

How Does Wi-Fi Work?

Basically, a Wi-Fi network works in pretty much the same way your cellular phone or TVs run by antennas. Essentially, it uses radio waves for transmitting data or information to and from your devices and the computer network or the Internet. If your computer wants to communicate with an Internet website and vice-versa, information is sent via your modem as efficiently as a wired connection. The secret here is the wireless middleman – the wireless router. It’s your device’s link to the modem, which is your gateway to the network and the Internet. It’s the wireless router that converts the data and information that passes through it into radio waves that can be received or understood by your wireless devices such as computers and gadgets, all of which use specific software and hardware for such a task. In the opposite manner, the wireless router converts the information or data passed on by your

devices into a form that can be interpreted or understood by the network or websites you’re accessing.

You may wonder if there’s any difference at all between your cellular phone and Wi-Fi network, given they’re both using radio waves. Well, there is. Particularly, Wi-Fi networks operate at significantly higher frequencies – between 2.4 gigahertz to 5 gigahertz (GHz) – while your phone operates beneath the 1 GHz level. Basically, the higher frequency allows for significantly more data to be transmitted over the airwaves.

Think of it this way – your home or workspace’s wireless router has the ability to link together multiple computers and devices without having to use any physical contraptions to establish such links. This provides a huge amount of benefits, particularly in terms of mobility. You can work anywhere in the house or office for as long as your Wi-Fi signal is able to reach your chosen area and either send your work to another person anywhere in the world via the Internet or print it using a Wi-Fi enabled printer that’s located in another part of the house or your office. Your wife can tap into the same network to watch cooking videos on her tablet while in the kitchen. Your kids can do their homework at the same time you and your spouse are accessing the Internet – all in the comfort of their bedrooms or another area of the house. The possibilities are endless!

Of course, Wi-Fi isn’t perfect – as with all great things. In particular, you still have one major problem: how to afford all those computers and gadgets for each and every member of your household or office. But then again, that’s not going to be addressed in this book.

Hot-What?

As mentioned earlier, places covered by Wi-Fi networks are referred to as hotspots or Wi-Fi hotspots. Without hotspots, there’s nothing to hack! And obviously, you don’t have to hack your own Wi-Fi, I hope (?). So that means you’ll need to find other people’s hotspots. Now how do you do that exactly?

Outside the home or office, hotspots are found in many public places such as cafes, hotels, libraries, airports and even malls! If you’re following people who are referred to as “warchalkers” – people who write the details of Wi-Fi networks they discover in public places on walls, usually in chalk, it’s easy to penetrate such networks. However, this may be considered as “unethical” penetration or hacking of Wi-Fi networks and in some jurisdictions, is punishable under the law. So be very wary about hacking Wi-Fi networks just for the heck of it. In the next chapter, we’ll talk about ethical hacking.

Chapter 2: Ethical Hacking (?)

If you had permission to enter or access a Wi-Fi network, you wouldn't need to hack into it now, would you? That being said, unauthorized hacking is obviously unethical, right? Well, not necessarily. Believe it or not, there is such a thing as ethical hacking, which is the proper application of what you'll learn in this book.

Essentially, ethical hacking and ethical hackers both refer to the type of hacking a person, or a firm does with the intention of identifying or exposing a Wi-Fi network's potential weak spots that can be used by the scoundrel hackers to wreak havoc on a network. In other words, ethical hacking is meant to make an existing network stronger by exposing its weak spots in order to fortify or strengthen them against external attempts at unauthorized access. Ethical hackers attempt to bypass networks' security measures in order to make sure such measures are foolproof and failsafe. If you are having trouble understanding this, imagine Floyd Mayweather's trainers or sparring mates doing their best to hit him where it hurts during training in order to strengthen his ability to defend himself against the second best boxers in the world.

It's obviously a great strategy as he retired undefeated after getting it on with the world's best boxers.

What Makes Hacking Ethical?

If you're going to use what is in this book to hack networks in an ethical manner, the following are the rules that you'll need to obey:

1. You’ll need to obtain expressed permission – often times written for your protection – to scan a network and attempt to hack it in order to identify potentially vulnerable aspects or areas that bad hackers can take advantage of to gain unauthorized access.

2. You have to respect and protect the network owners’ privacy as if it were your own.

3. When you’re done with hacking the network, you must ensure that your activities or work are properly closed out, so you don’t leave open opportunities for others – or even yourself – to breach the network at another time.

4. If you’re able to successfully hack into the system, you must inform the networks’ owners, the hardware manufacturers or the software developers about the weak or open areas that you were able to take advantage of that allowed you to enter the network without proper authorization.

The truth is, the terms “ethical hacking” and “ethical hackers” have taken a lot of crap from people who simply do not believe hacking can actually be an ethical or even noble occupation. For them, hacking is hacking just as murder is murder so that whichever way hacking is presented or pictured, people who hack ethically are automatically dumped into the same category as the cyber criminals and scoundrels.

But that is totally wrong. If not for hacking of the ethical kind, today’s networks would be totally unsecure and as such, wouldn’t have evolved or flourished as they have. If not for ethical hacking, network weaknesses and vulnerabilities can’t be discovered and strengthened, which wouldn’t allow the e-commerce industry to flourish and continue to flourish.

Now if you want to become a legit ethical hacker, you’ll have to get a certification. Yes, there’s such a thing as a Certified

Ethical Hacker – also known as CEH! And you can get such a certification from an organization called the International Council of E-Commerce Consultants or EC-Council (believe me, there’s nothing easy about that council). Be prepared to shell out $500 for the examination.

Chapter 3: Hacking It Like A Villain – WEP-Protected Networks

Now that you're oriented with the basic hacking terminologies, it's time to hack it like a villain for heroic purposes! And before you start attacking the walls of cyber-

Jericho, you'll first need to understand how Wi-Fi networks are protected or secured.
Wi-Fi networks send and receive data in terms of encrypted data packets. It's similar to when you're talking to a close friend in a very rare language in the presence of other people so that only the two of you can understand each other. Basically, these data packets come with encrypted security network keys, without which it's virtually impossible to access a Wi-Fi network. And if you get a hold of it, voila! – Complete access is yours!

When it comes to data encryption of wireless networks, there are 2 main kinds: wireless equivalent privacy (WEP) and Wi-Fi protected access (WPA). WEP is the very basic type of

encryption, which can be hacked easily these days, making it a relatively unsafe option for most Wi-Fi networks. But because not a lot of people are information technology (IT) experts, most Wi-Fi networks still encrypt data using WEP.

On the other hand, WPA is a more secure option between the two. If you want to crack or hack into a WPA-protected Wi-Fi network, you'll need to generate or make use of an extensive list of common passwords. In short, you'll need to go through the laborious process of trial and error in order to successfully hack your way into such a network. A variation of the WPA is the surprisingly named WPA-2, which is even more secure. Your chances of cracking into a WPA-2-protected network may be moderate if the network administrator assigned a fairly common or easy-to-guess password but if that administrator actually did his or her job well and used a strong password as well as disabling the WPA PIN feature, you might as well kiss your chances of successfully hacking into such a network goodbye.

And because WEP networks are relatively easier to hack, it’s the type of network we’ll focus on first in this book giveny ou’re a beginner when it comes to this type of thing. Otherwise, why else would you be reading this book? But no worries – we’ll also talk about hacking a WPA network later on.

The Tools Required

Your single most important tool will be a wireless adapter that’s compatible. Your computer’s wireless card or adapter needs to be compatible with the CommView, the software you’ll need to hack into a WEP-protected network. The importance of compatibility here is to ensure that your wireless adapter or card is able to get into “monitor” mode, which is very important when it comes to capturing data packets and hacking your way into the network. If you want to check your computer’s wireless card compatibility, you can go to http://www.tamos.com/download/main/ca.php for details.

And as you’ve guessed by now, the next important thing you’ll need is the CommView for Wi-Fi software. This is what you’ll be using to get the data packets from your desired networks’ adapters. To download CommView for Wi-Fi, go to http://www.tamos.com/download/main/ca.php.

Next, you’ll need another software to do the actual hacking or cracking of codes – the Aircrack-ng GUI. You can download it from http://www.aircrack-ng.org/ so you can install it too.

The setup

After you've downloaded your zipped copy of CommView from the site I've given you earlier, extract it and install the software by running "setup.exe". Once you're done and the software opens for the very first time, you'll be shown a guide for installing the driver. Simply follow the guide's prompts in order to successfully install your wireless adapter or card's driver.

Once you've successfully installed the driver, it's time to run the software. You can do it by simply clicking on the "play" icon, which you'll see on the application window's top left side. After you've clicked it, scanning of available wireless networks will begin. As CommView begins scouring for available wireless networks, it will generate a list of such networks together with their security and signal types. It's from this list that you'll choose your "prey" or target network for ethical hacking. Again, let me emphasize the word "ethical"!

Choosing Your Target

Now that you have an actual list, keep in mind the following things when choosing your network:

Since we're talking about hacking WEP-protected networks, it goes without saying that your choice of target networks is limited to such. Targeting WAP-protected networks is much more complicated for a beginner and as such, focus on getting this one first before attempting to hack WAP networks.
Choose the WEP network that shows the strongest signal.

Choose the WEP network that has the least decibel (dB) value.

After setting your sights on a network, select that network then click on "capture" to begin the packet capturing process from the channel you desire. However, it's possible that you'll see packets from all the other networks in a particular channel that you didn't choose being captured by CommView. When this happens, make sure to limit such captures to the chosen network only by doing the following:

Right-click your chosen network. Click "copy MAC address".

Click on the tab at the top that's labeled "Rules".

Choose "MAC Addresses", which is on the tab's left-hand side.

Click "enable" for MAC Address rules.

Select "capture" for Action and select "both" for Add Record.

In the box below, paste the earlier copied MAC address. Because you only need to get packets of data for hacking into the chosen network, select "D", which is located on top of your window, and deselect both M and C, which stand for management packets and control packets, respectively. And after you've collected the packets, you'll have to save them for hacking or cracking later. In order for you to do this, here are the steps:

Go to the tab labeled "Logging" to enable the software's auto-saving feature.

Limit the Maximum Directory's Size to only 2,000.

Make the Average Log File Size to only 20.

And now you wait. The length of time the software takes to get enough packets of data is dependent on how much the network is being used as well as its signal. For a pretty decent signal level, the software needs to get at least 100,000 data packets. When you believe the software has already collected that much packets, it's time to export those by doing the following:
Click on the "Log" tab. Once there, click "Concatenate Logs".

Choose all your saved logs and keep the CommView for Wi-Fi software open.

Then, go to the specific folder where your concatenated logs were saved and open the log's file.

Choose the format File-Export-Wire shark tcpdump and assign your choice of destination folder. Doing this will save your logs using the ".cap" file extension name to that particular folder or location.

And now, it's time to get hacking!

The Hack!

Remember the file Aircrack-ng that I wrote about earlier?

Well, if you haven't downloaded it yet, it's time to do so at http://www.aircrack-ng.org/ to get crackin' or hackin'! Then extract its zipped file, open its folder and go directly to "bin" to run the Aircrack-ng GUI.

Now that you're running the file, select "WEP" then open your saved logs with the ".cap" file extension name. When you've opened the file, click on "Launch", which will then show a command prompt. In that prompt, type in your chosen Wi-Fi network’s index number then wait some more. Assuming everything goes well, a wireless key will be generated, which is your access to the network. If not, the software may ask you to collect more data packets. If that happens, simply capture more packets and repeat the process until you get a wireless key. It’s that easy!

Chapter 4: Hacking It Like A Villain – WPA-Protected Networks

Given that WEP networks are quite easy to hack, as you’ve learned earlier, more and more network administrators or owners prefer to use WPA protection. This means if you stick to the earlier hacking section, your chances of successfully – and ethically if I may add – hacking into Wi-Fi networks will continue to go down. It is for such an ethical reason that I’m gonna teach you how to hack into WPA-protected networks.

For this task, you’ll need to download a copy of the free and open-source tool named Reaver. This program can help you take advantage of a particular breach or Achilles heel in the most wireless routers’ security system, which significantly boosts your chances of successfully hacking into WPA networks with relative ease even if you’re not a professional hacker. What you’ll need for this endeavor:

1. The Reaver program;
2. Blank DVD;
3. A Wi-Fi compatible computer; and
4. A couple of hours of free time.

For the Reaver program, you’ll also need the following:

1. BackTrack 5 Live: This program is basically a Linux distribution that is bootable. It’s packed with many tools for testing networks and will significantly make your ethical hacking task so much easier,

especially as a beginner. While this is optional, being a beginner makes this quite mandatory. And for the hacking procedures in this book, you'll need it so my apologies for even saying it's optional.

You can get the program from the download page of the website of BackTrack then burn it to your blank DVD (if you need an explanation on how to burn a CD, follow this link: http://www.wikihow.com/Burn-a-CD). In particular, choose "BackTrack 5 R3" from the drop down menu of "Release". Then, select "Gnome 32-bit", which is your safest bet as a beginner, then "ISO" for image before downloading the ISO.

2. A computer with a DVD drive and Wi-Fi: The beautiful thing about the program is that it works with most computers or laptops' wireless cards, especially the latest model ones, so no need to worry about compatibility here. And of course, you can't use a computer that doesn't have a DVD drive. So if you're using for instance MacBook air, good luck.

3. A WPA-Protected Network: In particular, you'll need a

   WPA network whose WPS feature is turned on. It's because this feature is what creates the Achilles heel in the security of WPA networks.

4. A virtue called patience: While using Reaver can make this 4-step hacking process much easier, it will take time. Why? Basically, Reaver is just an automated trial-and-error process that will try multitudes of possible password combinations in order to hack into a WPA-protected system. When you check out Reaver's home page, you'll find that it recommends setting aside a couple of hours. It may take less or more time, depending on the strength of the networks' passwords.

Now that you have the requirements down, it’s time to start hacking! Here are the 3 steps to hacking it!

Boot

Place your DVD containing the BackTrack program in your computer’s drive and boot using the disc. If you’re quite unfamiliar with live DVD and think you need more help, just Google it.

While the program’s booting, choose the boot mode, then choose “BackTrack Text – Default Boot Text Mode” before pressing your computer’s “Enter” key. Afterward, the program will boot a command line prompt, in which you’ll need to type the word “startx”. Press the “Enter” key.

Hack-attack Preparations

Before you can use Reaver, you’ll first need to know what your computer’s wireless card interface name is, your target network’s router BSSID (think of this as the router’s unique identification made up of letters and numbers), and set your computer’s wireless card in monitor mode.

First, let’s get your wireless card’s interface name. To do that, type “iwconfig” in the space labeled “Terminal”. Then, press the “Enter” key. After that, you'll be able to see a list of wireless devices. Chances are, your computer's wireless card interface name will be "wlan0". But if your computer has multiple wireless cards or a more complicated setup for networking, the interface name may be different.

Let's assume that your card’s interface name is "wlan0", you can execute or use this command to put your card in monitor mode: *airmon-ng start wlan0*. This command will produce the name of your monitor mode interface, which you must remember to copy. Chances are, the monitor mode interface name will be “mon0”.

Next, it’s time to determine the BSSID of your chosen target network’s router. This is for you to guide Reaver on the path it needs to take to help you get hackin’! To do this, simply execute this command: *airodump-ng wlan0*. If this doesn’t work, try using the monitor’s interface name in the command instead: *airodump-ng mon0*. Afterward, you’ll have access to a list of the available Wi-Fi networks in your area.

As soon as you see your target network’s name, stop the list from updating by pressing Ctrl+C, unless you’re willing to wait for it to stop. Then, copy your target network’s router BSSID, which is normally seen on the far left side. Under the ENC column, you should be able to see WPA or WPA-2 listed under it. If all you see is WEP, you already know how to hack such networks. If not, go back to the previous section in this chapter.

Armed with the interface name and BSSID, it’s time to use

Reaver to start hack-attackin’ – ethically of course!

Hack Attackin’

In the space labeled “Terminal”, replace “bssid” and “moninterface” with the BSSID and monitor interface name you noted earlier. If for example, the BSSID and monitor interface name is J9:ET:7X:69:EE:3G and h0ck, respectively (both of which are just made up), the command would then look like this:

```
reaver -I h0ck -b J9:ET:7X:69:EE:3G -vv
```

After typing the command, press the “Enter” key, sit back and relax. Now, the truly hard part here is to sit back and relax for hours – and I mean hours. It can take anywhere between 2 to 10 hours on average, depending on your target network’s password strength. This is because the program is an automated trial-and-error approach to trying multitudes of different password combinations. But then again, you can always do something else such as play video games, read a book, watch TV or sleep.

A few things about Reaver

While Reaver works well with most routers, there’s a small chance it may not on a selected few. As with people, Reaver is not perfect though it can perform very well in most cases. It also needs your target network to have a very strong signal to work well. So if the network you’re trying to hack is 10 miles away, you may want to consider moving a bit closer – 9.99 miles closer to be exact.

Oh, and part of Reaver’s imperfections is that there may be times that Reaver can be locked into a loop of using the same PIN over and over again or take a timeout while in the middle of the hacking process. Don’t worry. Just let it be and it’ll eventually get back on track without your assistance.

If you for some reasons or need to stop the process, simply do so by pressing Ctrl+C while in the middle of the hacking process. You don’t have to worry about restarting the whole thing again later on because Reaver will save all progress made until the point you aborted so that when you run the command again, it’ll just pick up where your hacking process left off. Just make sure that in between, you don’t turn off your computer. It’s because doing so while running a live DVD such as BackTrack tends to reset pretty much everything.

And my friend, that is how you can successfully – and ethically, if I may add – hack into a Wi-Fi network.

Chapter 5: Basic Hacking-ology Terms

Now that you learned basic hacking for beginners, I'm sure you'll want to study the topic on a much deeper level and learn more complex methods. While this book covers only the basic and easy ways of hacking Wi-Fi networks for beginners, I want to help you prepare well for more advanced techniques by giving a list of some of the most common hacking terminologies you'll encounter as you progress in your ethical hacking efforts. If you are familiar with these terminologies I recommend going straight to the conclusion.

Adware

It's basically software that forcibly displays ads on a system, some of which are malicious to the point that it pops up ads so frequently as if it's already running your system.

Back Door

A network or computer system's entry point where hackers – such as yourself – can circumvent security systems to gain
unauthorized access. Normally, system programmers or developers – in order to access systems or programs quickly during the development stage – create these back doors. The problem lies when they forget to lock the door after the development is complete.

Bots

These are software "robots" that automatically perform a wide range of tasks. Firms like Google use these in order to comb through millions of websites in order to search for relevant content based on the keywords used for searches. Such bots aren’t intended to cause systems harm but rather to just help people perform relevant searches on topics they’re interested in. But these bots also have their evil twin siblings, which are used by unethical hackers to cause harm.

Cookies

A small information packet from websites that you visit that is stored in your computer system. These are normally used to help personalize the information sent to you – often for marketing purposes. For example, if you visit a website that always requires you to fill out forms, cookies help you out by storing such information, so you don’t have to fill them out each and every time.

Denial of Service (DOS)

It’s an attack that’s meant to make a website inaccessible or crash by overwhelming it. This happens because DOS’ automatically stresses a system with sheer frequency and number of “website visits” and data packets that are designed to stress it.

Dumpster Diving

This refers to the act of scouring through a personal or business computer or system’s “trash bin” with the intention of getting potentially useful personal information for pulling off cybercrimes. Truly, another person’s trash can be other people’s gold mines!

Easter Eggs

These refer to surprises installed by developers in a program or even on a circuit board. Fortunately, these are non-malicious programs such as a signature, text greeting or a short video. Keep in mind that Easter eggs are entertaining, not obvious, and reproducible in similar devices and of course, not malicious. Otherwise, they aren't Easter.

Firewall

This refers to a computer system or network's security barrier, which is designed to keep unauthorized users from accessing the system while allowing authorized ones to communicate easily with the system. Firewalls can be physical, software or a joint venture between both types.

Keyloggers

These refer to programs that were created for the purpose of record or to log each and every keystroke done in a computer. Such information is usually saved as a file on the same computer or collected and sent to another one within the same network or through the Web. This, however, runs the risk of unauthorized access by unethical hackers, which can be used to figure out a computer or a network's password for unauthorized access. These are considered to be spywares or software that are used for spying and getting confidential information.

Malware

This is what you call malicious programs that can be very, very harmful to your computer or network. Malware includes viruses, Trojans, worms and any other malicious programs of the same effect on computers and networks. The part of such programs that do the dirty and destructive work for which malwares were designed is called the payload.

Phishing

A method by which unethical hackers are able to obtain sensitive information from computers and systems. Usually, the phishing activities are conducted via emails that seem to be “legit” – looking as if they came from trustworthy companies such as eBay or PayPal. Such emails contain links that direct you to very attractive or interesting website only after you verify your account information. When you verify your account information, you essentially give unethical hackers, more popularly known as “black hats”, the opportunity to steal your identity and carry out cyber-crimes on your behalf.

Rootkit

In the Information Technology (IT) industry, one of the scariest things that can happen is an undetected hack into systems or computers. Detected ones provide opportunities to cut losses, minimize damage and strengthen the system. With undetected ones, hacking continues unchecked. Rootkits are the primary means by which black hats are able to pull off these types of stealth intrusions.

Spam

These refer to emails that aren’t solicited. In other words, these are unsolicited emails that you really don’t want to receive and are thus considered to be junk email. Often times, these are for marketing products or services but the scarier versions are those used for phishing.

Spyware

This is software created to collect information about a computer or network user without his or her knowledge. It can be as simple as tracking a user’s Internet browsing habits for purposes of smarter and more focused advertising. If you encounter pop up ads about products or services that are surprisingly in line with your interests, that’s a typical example of spyware.

Trojans or Trojan Horses

Consistent with its name, these refer to malicious programs that are made to resemble harmless and valid ones so that you will gladly accept or install them in your system, and open them. But just like the original Trojan horse, it contains destructive files that can steal information from your computer or system, destroy your files or even wreck your computer or network. A Trojan’s power lies in the fact that you gladly let them into your computer or network thinking it’s a legit and harmless program, and the worse enemies are those that come from within.

Worms

Self-contained but destructive malicious programs that have the power to replicate or multiply itself. It also doesn’t need to ride on another program or file to enter and wreak havoc on a computer or network – it can copy and move itself between computers or systems by itself without the intervention of users or administrators. While it’s not as destructive as

Trojans, it can significantly slow down the performance of most computers and networks if not effectively isolated or removed.

Conclusion

Congratulations. You're now armed with the knowledge of how to hack Wi-Fi networks. But knowing is just the tip of the iceberg – the main part lies with the implementation of what you've learned. As such, I encourage you to apply what you learned here as soon as possible. Otherwise, you run the increasing risk of not being able to hack Wi-Fi networks successfully.

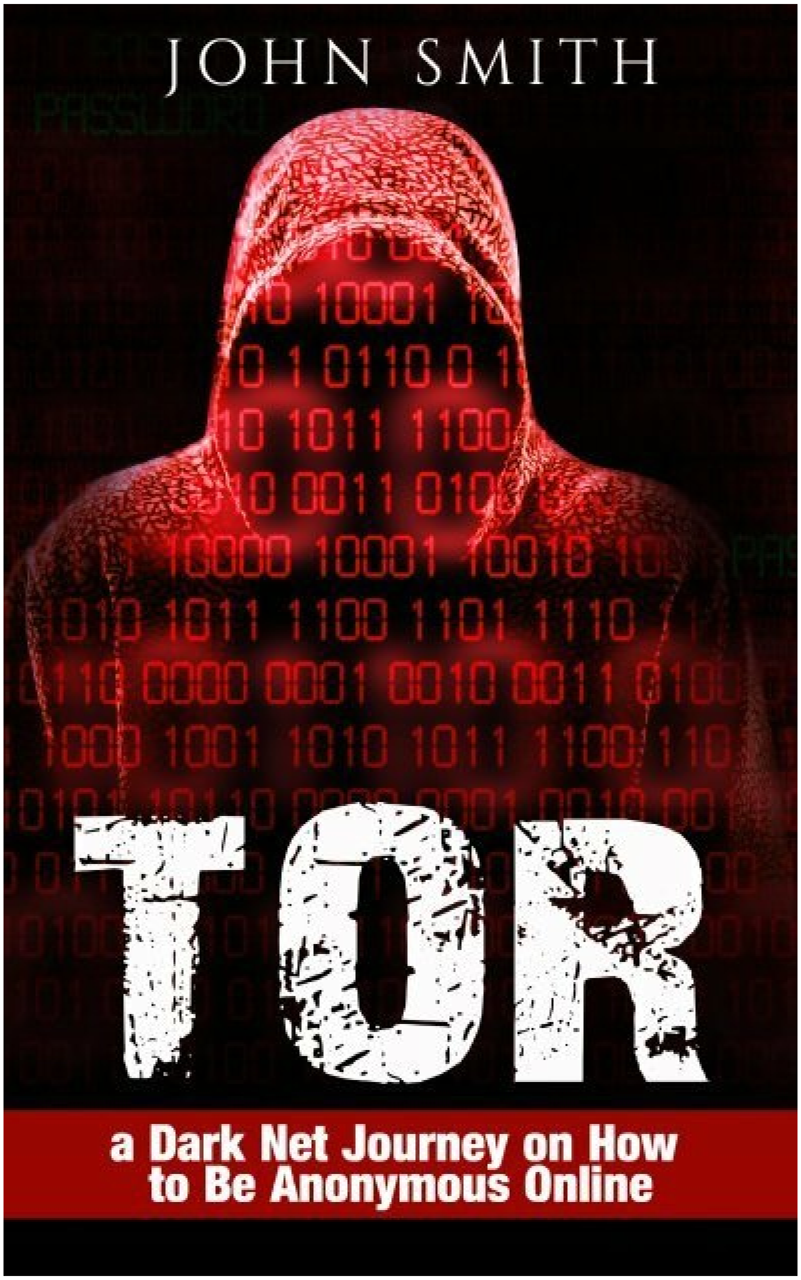
I recommend starting with your personal Wi-Fi network at home. That way you don't run the risk of being caught or worse, sued. And more importantly, keep in mind that hacking should be done ethically – with permission and great care. Otherwise, don't do it. This book is meant to help you strengthen your or other people's computer systems or networks – not to wreak havoc on them. This book is about helping others, not bringing them down.

If you enjoyed my book or found it giving in any way, would you please leave a review on amazon? I would be most grateful, and it would be an incentive for me to publish more books on this topic. Just swipe to the right one more time and you will be able to leave a comment.

PS!! If you are interested in learning how to surf the web **anonymously** or how to access the **DARK WEB** then you should check out my book on the topic. I have attached a little preview of the book's content below.

ASIN: **B01MY6ANCK**

URL: http://amzn.to/2juBmFS


JOHN SMITH
TOR
a Dark Net Journey on How to Be Anonymous Online

TOR

A Dark Net Journey On How to Be Anonymous Online

John Smith

Introduction

In the recent times where such issues like doxing and swatting (check meanings below), and even premature exposure of your details or identity have been on the rise, there has been a growing demand and need for online anonymity.

All the same, everyone needs it; whether it's about protecting your identity, not because you are doing anything questionable or illegal but mainly because you want social safety (especially if you are an introvert in an online community); you need to be invisible, alone and feeling safe with the best tool to help you achieve all that.

Do you often experience personal harassment that constantly denies you the freedom of expression? Or is the thought that 'anything you say or do online may be used against you' so crippling such that you limit yourself? Well, the good news is that there is hope; you can limit what anyone out there could know about you by using tools specially designed for guaranteeing your anonymity. One of the best tools of this kind is TOR.

With this book, you'll learn everything you need to know about TOR- a free software and also an open network that will defend you against network surveillance threatening your personal freedom and privacy, traffic analysis, business activities and so much more.

ASIN: **B01MY6ANCK**

URL: http://amzn.to/2juBmFS