Author: Kharim Mchatta

Article: Cybersecurity Careers

Date: 15/9/2021

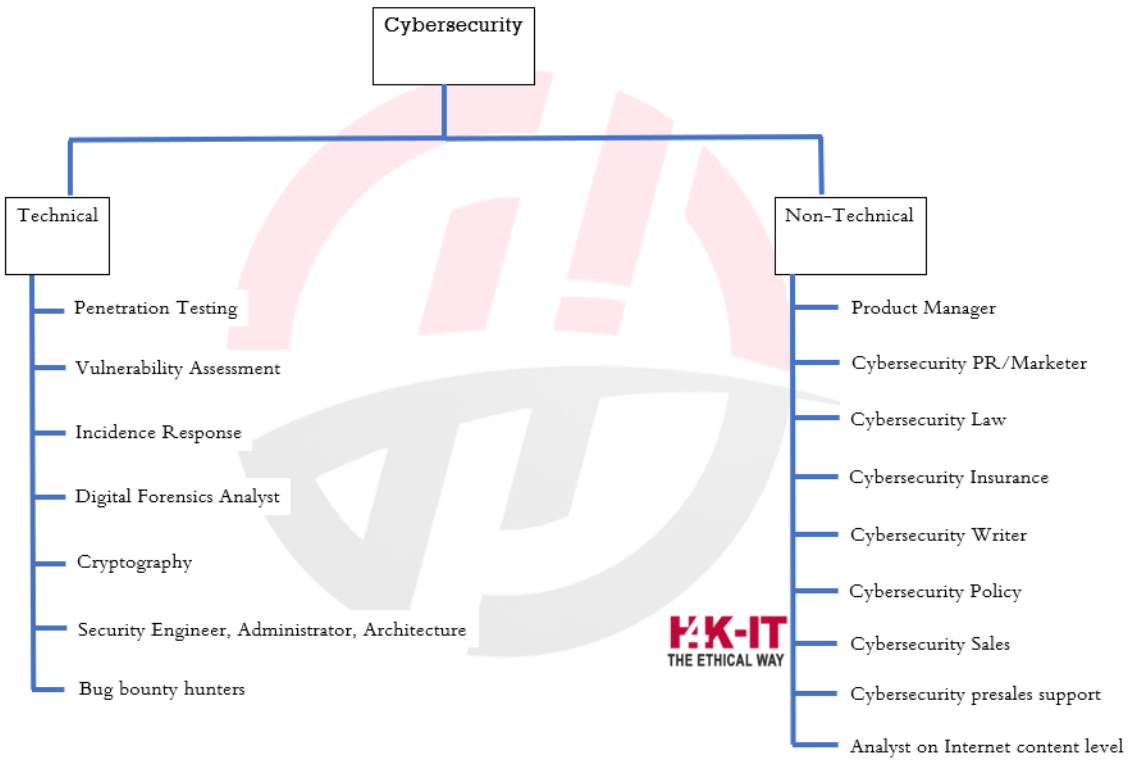
CAREERS IN CYBERSECURITY

A misconception that a lot of people have about this industry is that cybersecurity requires an individual to be a tech savvy in order to strive in this industry, partially is correct but it is not entirely true.

Another misconception is that cybersecurity is a single field (example accounting or human resource (HR)) which someone can learn, this is far from the truth, cybersecurity is split into branches, where under those branches, they are split further to subbranches which an individual concentrate's on as their career line.

Most cybersecurity professionals would pick a subbranch which they would tend to focus on, but on the other side they would know the basics of other area's relating to the main branch they picked

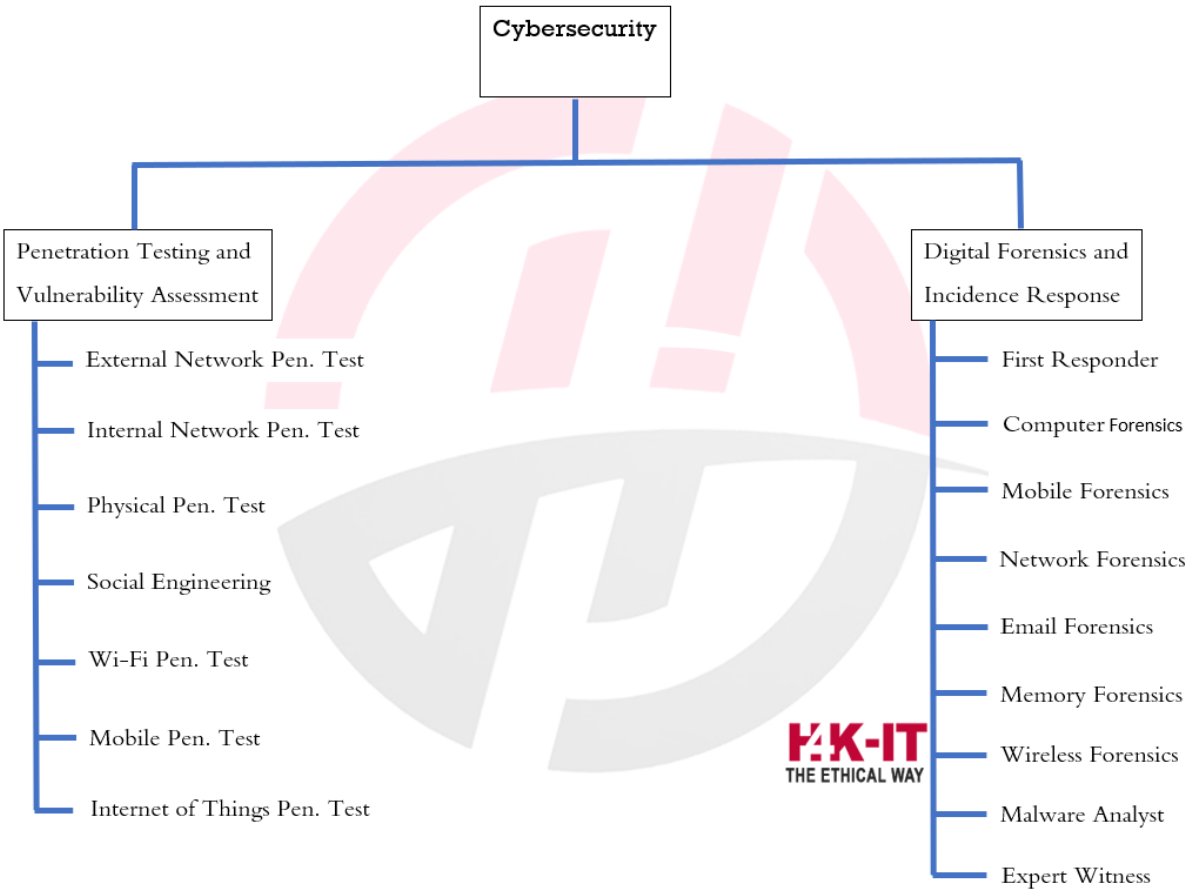
Cybersecurity as an industry is split into two major categories as shown in the below image



The most popular category in cybersecurity is the technical area. In this category is where an individual is required to be a tech savvy and know generally how computers work. The most famous career in the technical category includes Vulnerability Assessment and Penetration Testing (VAPT), Digital Forensics and bug bounty.

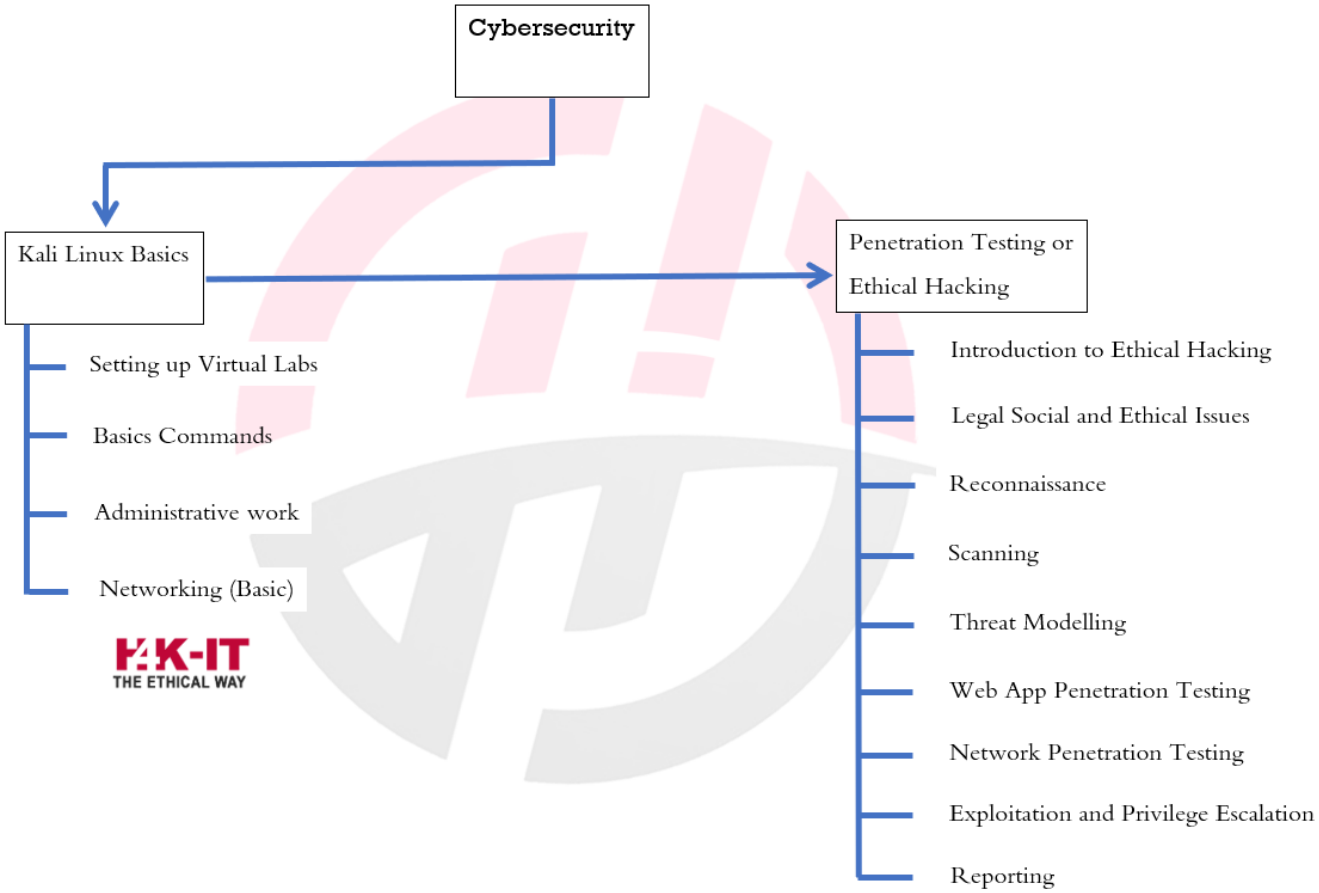
The less popular career in cybersecurity are found in the non-technical area. These careers are not popular simply because they don't involve doing any of the technical things which a lot of people find interesting and fun.

Going further in the technical area, using Vulnerability Assessment and Penetration Testing and Digital Forensics and Incidence Response as an example we can see that these careers have been broken down further into specific area specialization as shown in the image below.



If an individual wants to focus on Penetration before anything they need to have a basic understanding of Kali Linux as an operating system for many cybersecurity professionals, then they can go and get started with ethical hacking.

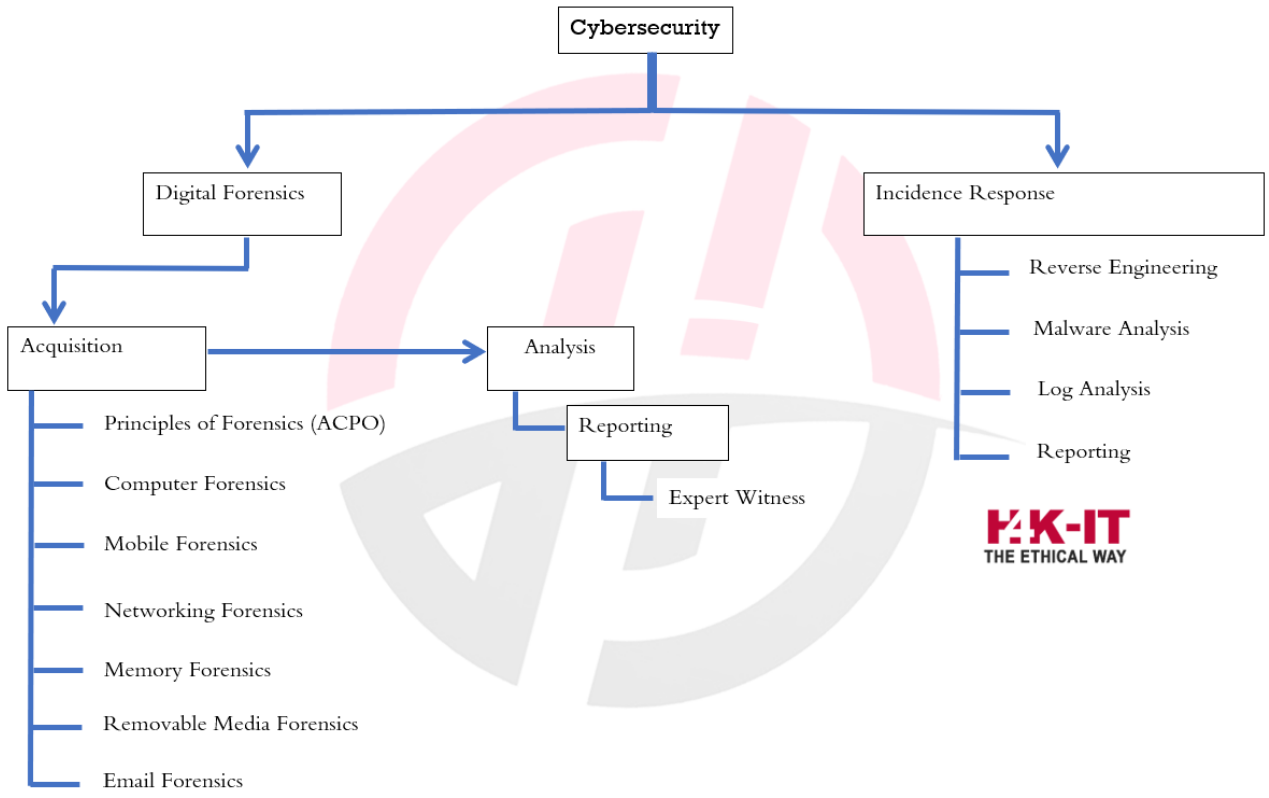
The below image shows the things an individual needs to learn and where they need to start from.



Going to digital forensics as a career path, this field has a lot of sub careers which an individual can decided to focus on. One can decide to solely focus on just performing acquisition, either generally on all area's or on a specific area (Computer acquisition, Mobile acquisition, network acquisition etc), the other person can decide to focus on just doing the analysis. Analysis basically covers doing the investigation after an image has been acquired. The other individual can decided to become an expert witness. An expert witness is the individual who goes to present the evidence in the court of law.

Another career in digital forensics is First responder. A first responder is basically an individual who arrives first in the crime scene and is the one who is responsible to secure the crime scene, take photos or videos of the crime scene and acquire the evidence to send it to the forensics lab.

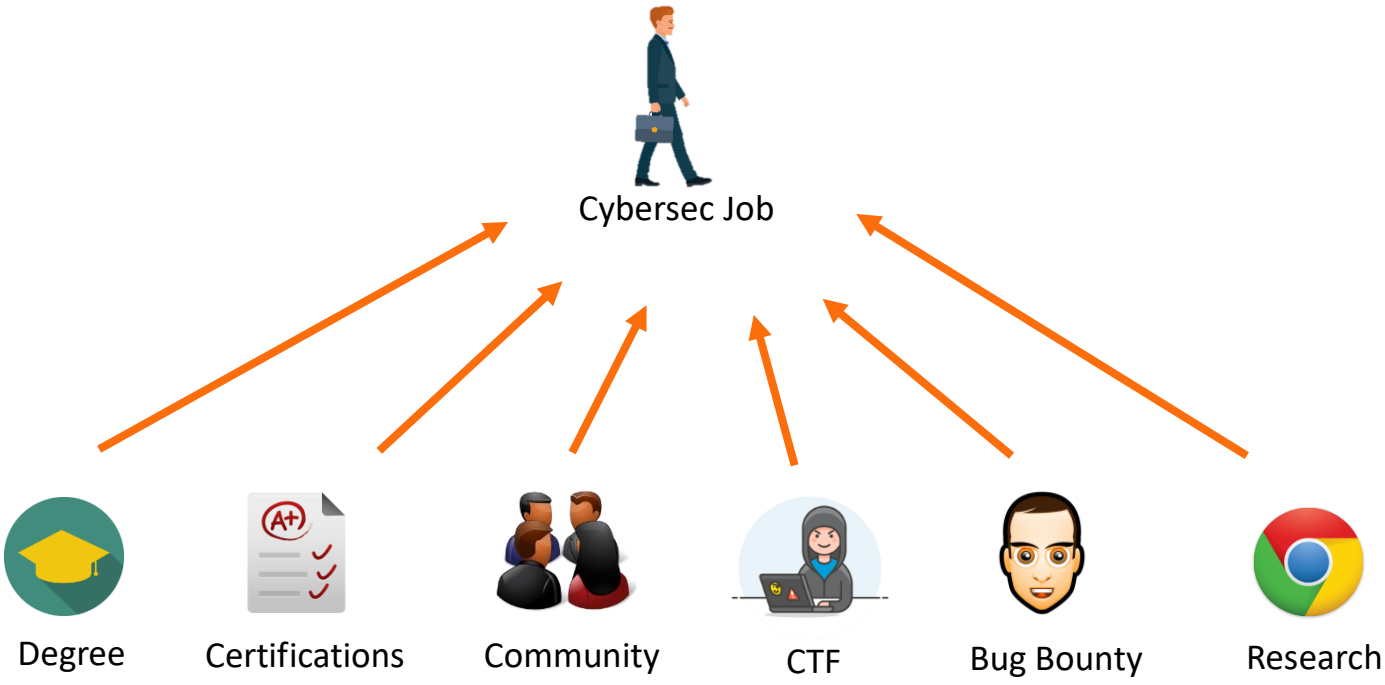
The below image shows all careers that are available in digital forensics and incidence response in which an individual would want to pursue.



ENTRY ROUTES IN CYBERSECURITY CAREERS

The analogy for people who have not yet started into cybersecurity is in order to get into this industry you have to have a cybersecurity degree, well this is far from the truth, there are a lot of cybersecurity professionals who don't have a cybersecurity degree, but they are in the industry, others have made a complete switch of career and got into cybersecurity.

Below is an image that shows different routes of getting into cybersecurity



As shown in the above image there are different ways on which you can get started in the different careers in cybersecurity

- Degree – This is the most common method which a lot of people use to get started into cybersecurity, they get their bachelor's degree where they are taught about cybersecurity.

- Certifications – Other people don't want to use the degree route due to the number of years required to simply get a degree, so they opt to go and get a professional certification like CEH or OSCP etc.
- Community – Here is where an individual joins a cybersecurity community and gets access to different learning materials and learn from members of the community.
- CTF – CTF's are cybersecurity game where an individual can practice their hacking skills legally. Some individuals prefer to have hands on experience then decide to do CTF's for learning purposes.
- Bug bounty – bug bounty are programs where cybersecurity professionals help companies look for vulnerabilities in their systems in return, they get paid depending on the bug they find and the severity (impact) the bug has to the system. A bug bounty hunter is basically a freelancers
- Research – This basically covers personal learning. This is where an individual goes to the internet and study different learning materials which could range from either reading CTF and Bug bounty reports to learn different hacking techniques and methodologies and others would go and watch videos on YouTube and others would basically join online courses from different platforms like Cybrary or Udemy etc.

As you can see there are different ways on which an individual can use in order to gain the relevant experience and knowledge needed to get a cybersecurity job, the beauty of cybersecurity as an industry is that any skill that you have acquired in your previous role would be useful example if you were a system or network administrator, the skills you obtained from that role are going to be useful.