MULTI-SOURCE RESEARCH PAPER

Du Jinrui

November 23, 2022

It happened when I was still a teenager, wandering around a trail in a mid summer afternoon. Suddenly, I found a road leading to a wider area. Different from the trail, the road was well conditioned and the trees on the sides were taller and tidier. As I happily followed the road, expecting some beautiful sights, viola, it was the door to a military base. The sentinel asked me to leave before I entered the fifty meters perimeter. I was angry, frustrated. Philosophers wrote so many arcane texts on freedom, but call me childish and selfish, to me, my freedom was breached when I was stopped from entering the military facility. I was upset that such boarder exists: we need a passport for going to another country, house owner's consent to enter the private property, password to access protected websites. It seems that freedom and power come hand in hand. If I was the president of the country, I would be entitled to enter the base as I like without anyone stopping me. Luckily, there is still a space that is more free than the real world — the cyberspace. Admitted that such constrains also exist in the cyberspace, as ordinary people who are not powerful, we feel much more free in the cyberspace. We could conspire against the government using secret communication channels. We could deface targeted website to promote our own values (Holt, Bossler, & Seigfried-Spellar, 2017, p. 21). We could do anything we like without constrains in this space — if we were outlaws. However, we are good citizens, we admit that in order to secure the freedom of all, we concede part of our freedom to the government. But sometimes, we have to understand the outlaws, their capabilities and psyche, to better protect ourselves. Having been a software engineer for more than three years, I will try to tackle the question: how to become a skilled criminal, or a skilled cybersecurity professional. I will argue that in order to become a hacker, one will need to have both hard skills and soft skills. In the first part of this essay, we will explain the essential computer skills, discussing why programming, mathematics, and the knowledge of computer science are important. In the second part of this essay, we will talk about the required people skills: rapport building, and body language. It is important to note that my experiences and studies are limited, still I hope to provide a general skill map that you would find valuable by the end of this essay. Let us start by presenting an important factor why teenagers can become hackers, after all, these hard skills are not easy to acquire.

There are hundreds of computer vulnerabilities found every day (Holt et al., 2017, p. 86), therefore when security professionals search for these flaws in a computer, they will not do it manually, instead, they automate the process by making software. Lots of these software are free to use. Imagine that a kid just watched a hacker movie, and thinks that it is so cool to hack computers, then downloads one of the tools and attacked a website. These kids are not hackers. In the hacker subculture, they are called "script kiddies", or "wannabes" (Holt et al., 2017, p. 116). In the hacker subculture, "knowledge" is a key value, meaning to have a deep understanding of the computer software and hardware, and to solve problems in innovative ways (Holt et al., 2017, p. 130). Having talked to many fellow software engineers and seen many college curriculum, for example, courses from CMU (Carnegie Mellon University, n.d.-b) and SANS Institute (SANS Institute, n.d.), I know that there are some subjects one must study in order to have a solid understanding of computers. They are: operating systems, computer networks. Why they are important? For example, criminals can download the Tor browser to hide their locations then sell child pornography. Its anonymity nature forces FBI agents to hack the Tor infrastructure to obtain information (Holt et al., 2017, p. 311). I am not an expert but it is reasonable to assume that the FBI hackers have the knowledge that is taught in any cybersecurity degree curriculum, otherwise they wouldn't know how to do it.

Beyond the curriculum, programming skill is also a must if you want to develop your own tools for hacking and have a deep understanding of computers. Which programming languages to learn? It is an age old question and the answer is more of an opinion rather than argument. A typical answer is we should learn five languages (Raymond, n.d.). Two languages that are prevalent and easy to use. At current time, they are Python and JavaScript. Two languages that are the backbone of almost every system: C and C++. And learn one more language for enlightenment: Lisp or Haskell. There is also necessity to learn the Assembly language if one truly wants to dig into what is going on under the CPU board because it is the language most close to the binary code.

Now, mathematics. If someone want to be viewed as asexual, geeky, then math is a topic to bring out to the table. To defend ourselves, we say that math is behind everything. It is the reason we can send people to the Moon, build towers that reaches the sky. It is also the reason why malicious hackers won't easily hijack your private messages sent through email — they are encrypted through modern cryptography. To have a grasp of cryptography, one needs to have basic knowledge of linear algebra (Hoffstein, Pipher, & Silverman, 2016, p. v). Depending on how much a person loves math, one can choose between a multivariate calculus based linear algebra or linear algebra without a calculus component. However, most colleges only offer calculus based linear algebra. Discrete mathematics being an indispensable component of every computer science curriculum is also invaluable.

We have touched upon the essential, or minimum requirement for a skilled hacker. And these requisites are all hard skills, taught in universities and colleges. However, it's the soft skills that really make the difference. Ageism is a thing in tech, largely because young people are deemed to be flexible, quick learners, and can work more hours. But soft skills grow with age. The more you experience, the more you understand people. Thus it becomes hackers' major competitive advantage. So what do I mean by soft skills? I am referring to social engineering. Have you ever received an suspicious looking email that has a link for you to click? Have you ever picked up a scam phone call? Then you may have been a victim of social engineering. In his book *Social Engineering: The Science of Human Hacking*, SE expert Christopher Hadnagy arms us with knowledge from his years of experience, providing a landscape of social engineering. I want to draw contents from his book here.

In the fifth chapter *I know how to make you like me*, he teaches us how to "build a bridge for communication based on trust and common interests" (Hadnagy, 2018), in other words, how to build rapport with people. I won't list every detail about the methodology. Instead, I want to show you how he used this skill to prevent a crime. The story begins with the law enforcement noticing an "OilHater" posting his speech online threatening to blowing up fracking stations. Chris then pretend to be interested in the oil industry, asking questions about the oil stations in the forum. A few weeks later, the OilHater answered one of his questions. From then on, they have more and more conversations. Chris agrees with the OilHater, saying that he also have a kid, and he didn't want the oil company to harm the environment in which his child is living. As they get closer and closer online, Chris gave the OilHater his fake name and address, in turn the potential terrorist offered to start an operation that would blow up an fracking station together with Chris. After Chris got the address and time of the meeting, the law enforcement successfully caught the guy.

Chris also worked with Dr. Paul Ekman, the rock star in the field of nonverbal communication. He mentioned through out the book how fundamental is it to understand the body language and how it helped him in many impersonation tasks. Since it is a popular subject, I won't go into detail. Anyone who is interested can pick up his book and read.

Some people may argue that they are not aspiring hackers, they do not need to study these things. My response is that, these skills transferable, universal. For example, we may not need to become an expert in computer networks and operating systems, yet computer literacy is a must in this modern society. You may not need to learn five programming languages, but even primary school students are starting to learn Python. Not to mention mathematics, where calculus is a required freshmen year subject in the United States. Soft skills, like building rapport is helpful when you want to negotiate for a salary raise (Voss & Raz, 2016). Studying body language increases your ability to identify people's emotion and helps you to become a better lover, parent, and friend.

Some people may question my motivation. Since I mentioned how I was blocked by a sentinel from getting inside a military base in the beginning of this essay. They might say that it is morally wrong to want to become a powerful hacker for this stupid reason. But don't forget that, being powerful is the way to awe your enemies. Having the ability to destroy but choose not to do so is the real virtue. Think about the story of the Sweeney Todd, he had a beautiful wife until she was unjustly taken and prosecuted by a powerful man. If somehow we could get dirty secretes of the villein, like the founding father of the FBI who had dirty secretes of presidents and senators, then his wife would be under our protection.

Some people may argue that you will never become a hacker who is good enough to infiltrate a military base. Plus, it is just too dangerous: what if the nation wants you to become a cannon fodder, or a company enslaves you because it has evidence of you doing illegal hacking years ago. These are legitimate questions but rare events. All I can reply is to be familiar with the legal issues. Do not do illegal things unless you have good reasons. And, protect yourself.

In this essay, I have tried to provide a training map for becoming a hacker based on my limited knowledge, emphasizing important aspects of both hard and soft skills. One may want to become a hacker for different reasons. For a man, he may want to protect the freedom of his loved ones. For a country, it may train hackers to counter cyber terrorism, digital piracy, and child pornography to protect the freedom of its people. One remaining question is how to train world-class, top-notch hackers? To answer this question, I'd suggest to study the way CMU educates its students. Their team has a leading record in the DEFCON CTF (Carnegie Mellon University, n.d.-a), the Olympics of hacking. Remember, the definition of a hacker could be a person who have a profound knowledge of any domain, and can solve problems creatively. So, we all have the potential of becoming a hacker!

References

Carnegie Mellon University. (n.d.-a). *Cmu crowned hacking champs at defcon27.* Retrieved from `https://www.cmu.edu/ini/news/2019/defcon-champion20191.html`

Carnegie Mellon University. (n.d.-b). *Information security (msis) - information networking institute - college of engineering - carnegie mellon university.* Retrieved from `https://www.cmu.edu/ini/academics/msis/index.html`

Hadnagy, C. (2018). *Social engineering - the science of human hacking.* New York: John Wiley Sons.

Hoffstein, J., Pipher, J., & Silverman, J. H. (2016). *An introduction to mathematical cryptography* - (2nd ed.). Berlin-Heidelberg: Springer New York.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and digital forensics - an introduction* (2nd ed.). New York: Routledge.

Raymond, E. S. (n.d.). *How to become a hacker.* Retrieved from `http://www.catb.org/ esr/faqs/hacker-howto.html`

SANS Institute. (n.d.). *Foundations: System architecture, operating system, and linux.* Retrieved from `https://www.sans.org/cyber-security-courses/foundations/`

Voss, C., & Raz, T. (2016). *Never split the difference - negotiating as if your life depended on it.* New York: Random House.