Not unlike asking 100 anarchists "how do you define anarchism?" if you were to ask 100 hackers how they would define a hacker, you might get just as many answers. I am a longtime anarchist, but someone who would only recently and reluctantly called themselves a hacker. So keep in mind that this is just one dude's (skid's) opinion about what a hacker is. If you disagree, that is fine. If you think that the definition of a hacker should be more nuanced, that is also fine. You should write your own article next time! For this essay, I propose the following definition.

A hacker is anyone who figures out solutions to problems using the tools available to them.

Ideally, the solutions to these problems would be elegant, but sometimes a quick and dirty hack that works is worth as much as a perfectly polished exploit. I am not going to get into a semantic discussion about " crackers versus hackers" - for the purposes of this column, the color hat worn by the hacker is entirely irrelevant. I don't even think it is necessary to limit this definition to computers. In the end, when one finds a solution to a problem, or gets the desired result, the question of "how" is not that important. Sure, it can be tremendously interesting, but does it really matter why something works or that it works? Put another way, do you need to know how a particular exploit works against a particularly vulnerable system, or simply that it works?

Rather than have a restrictive definition of a hacker that involves compromising vulnerable computer systems, I would rather have a larger definition of a hacker to encourage more people to start thinking critically. Life is too short to try and act as arbiter of a term, policing people's language about how they choose to define themselves. Our world has too many bullies in it, and anyone who would bully someone about how they define themselves is an asshole I don't care about. If your first reaction to someone calling themselves a hacker is to sneer and try to prove that they aren't, you need to take a long, hard look at yourself. I will return to the gatekeeping issue later because I think it is really important.

I became a hacker because of a series of happenstances. Let's start with professionally. After being burned out working as a network administrator for my hometown community college, I moved across the state - first to earn a BA and then a graduate degree in a subject (history) that gives me basically two options: either go earn a Ph.D or teach at a high school. Since I didn't get accepted to any of the doctoral programs I applied to after finishing my MA, and I was unable to find any academic work, I decided to start using Linux before going to college and have been using it daily for nearly a decade. So when it came time to start using Kali Linux for a touch of the ultraviolence, I knew how to get around the command line. I spent a few months teaching myself the basics in a really poorly constructed lab environment and asking my mentor a ton of questions. I even found a client that let me poke around their website. After that, a company nearby offered me a junior consultant position and I took it. Next thing I knew, I was getting paid to try to hack into banks and other businesses - a dream come true for the kid who grew up watching the movie Hackers and thinking that there could be no cooler job then getting paid to hack all day.

So when I mentioned earlier that a hacker is anyone who figures out solutions to problems using the tools available to them, let me give you a practical example. I was at a client's site (in this case, a bank) and we were doing a little physical recon as we were leaving the building. In hindsight, we should have done this when we first came in, but that is not the point of the story. The point is that I discovered two potential vulnerable spots in the client's network based on weaknesses I knew about because of my time first at the help desk and later as a network administrator. So when I say that gatekeeping is a problem, this is part of what
I am talking about. Just because I didn’t know how to really write code at the time, or develop my own exploits, I could have still leveraged previous IT knowledge to compromise the network in a way that someone who only has development experience wouldn’t know.

So even though I’m not in the best position to offer a message to aspiring hackers, I’m going to do it anyway. First of all, you have to be willing to fail. Often. When I popped my first shell on a client, it was using an exploit that failed four times before finally working. Information security as a field is one where you are simply going to fail. One dirty secret that professional penetration testers and red-team people hate to admit is that blue teams are good. They are often really damn good. Just because you are able to pop a shell, that doesn’t mean it will stay alive. Or that your connection will stay alive. If you want to be good, you have to first be willing to admit that you suck. Perhaps worse still is the knowledge that you are going to suck for a long time. Let me give another example.

I started the PWK course offered by Offensive Security, you know, “Penetration Testing with Kali Linux?” Anyway, going into it, I didn’t have a ton of programming experience. I’d taken a few classes at the aforementioned community college, one or two on UNIX programming at another school, and have been teaching myself Python for the last few months, but I am not a great coder yet. I still have a ton to learn.

Going through the course, you are expected to be able to write scripts and do the basics of exploit development. While these things are both fun, they also require you to fail, a lot. Anyone who has written code can tell you that your code is going to fail. You will figure out new and unique ways to make it crash and burn, but baby, it is going to burn. I’ve written code that borked machines so badly it crashed both the virtual machine and the host that was running it.

To paraphrase Jake from Adventure Time, sucking at something is the first step to getting good at something. In infosec, as in life, you have to crawl before you can walk.

So in addition to the message above, get used to sucking. The next bit of advice I would give to the aspiring hacker is to find a mentor: someone who knows more than you, and can point you in the right direction when you get stuck. Setting up a decent practice lab can be a pain in the ass. Having a mentor who can help walk you through it and give you nudges when you get stuck is worth its weight in gold.

Third bit of advice: Google is your friend. Perhaps, secretly, more than a friend. Sure, you have to cough up some of your personal data, but really, it’s the price you pay for the best search engine. You can find all sorts of cool stuff by using the right magic words.

Fourth bit of advice: get ready to fail more.

If you are willing to fail, be rejected, do some Googling, and you are fortunate enough to find someone to point you in the right direction, you still have a mountain of work to do. Even though hackers can sometimes have reputations for being lazy, the reality is that many awesome hacks are awesome because they save you from having to do more work.

Near the beginning of this article, I had mentioned that I would talk about a few reasons why I thought that gatekeeping is bad. I want to expand on this further, because I think it is worth talking about. Information security, as a professional field - if you believe the hype and what you would read online - is desperate for people. Warm bodies who can do anything from working in a SOC (Security Operations Center - monitoring alerts, tweaking firewalls, and overall trying to ensure that the networks they are watching over remain secure and uncompromised) to penetration testing, exploit development, reverse engineering, threat hunting, malware analysis, bug bounty hunting, and even more - the information security subsection of the information technology field appears to be growing and shows no signs of slowing.

What this means is that, like it or not, there are going to be more people coming into the field. Some people take the hard line with newbs and skids and won’t want them to feel welcome. Hazing and trials-by-fire still exist as well, but I don’t think that this is the best way forward. If we all want to get better, having more people to bounce ideas off of is the best possible outcome. Most free and open-source software advocates are aware of the many eyes theory, but if you aren’t, the idea is that many eyes make shallow bugs. Put another way, the more people that can look at code, the more likely we all are to find vulnerabilities that can then be patched. Or, the more people in information security, the better we can all get, regardless of the color of your hat.

Good news everyone! Systems will remain unpatched! There will always be some “business need” for old software, super old
hardware and operating systems, and stuff that just should not ever touch the Internet to be totally touching the Internet! Sysadmins and netadmins will insist that for “reasons” they can’t patch their stuff, at least not immediately, because ya gotta test patches! So, while they test patches, their vulnerable shit is just sitting on the Internet one quick Shodan search away! Plus, with the expansion of the Internet of Things (IoT) even more stupid shit will soon be touching the Internet, and IoT has a bad reputation for considering security as an afterthought, if they even think of it at all. That means that there will be more microwaves and smart light bulbs to pwn going forward!

What I’m trying to say is, there will be work in information security for a while to come, at least until machine learning and AI puts us all out of jobs (and hopefully just that and not, you know, killing us). Hopefully by then, the need to do 40 hours of work per week will be eliminated, and we can spend more time doing cool shit rather than spending a third of our day at work.

Until that day comes, try to be nice to newbs, skids, and scrub. Remember that everyone started somewhere. Most people didn’t begin writing exploits their first day, or even their first week. While I am sure that there are some who did, most had to rely on the work of others to learn. If you are in a position where you are more experienced, perhaps consider mentoring someone who is new. If you would rather not interact with a person, you could think about writing blog posts or doing video tutorials, which might end up leading to someone reaching out to you. There are also professional reasons why doing such things can be good for your career, if you want to reach the next level. Or, if you just want more Twitter followers, that can be a good avenue as well.

Remember, if you want to be a hacker, you can totally do it. It won’t be easy, you will fail over and over again, but you will learn almost certainly more then you ever expected you would. Not only about computers, systems, and networks, but also about people. Remember that some will shit talk along the way. There will be nay-sayers, haters, and you might make an enemy or two regardless of the color of hat you decide to wear. Until we can overthrow the capitalist system, we must have jobs. Being a hacker can either be an awesome job by itself, or be a framework you use to help make your life easier. Either way, if you figure out solutions to problems using the tools available to you, then you too can be a hacker. Bonus points if other people consider you a hacker too, but who cares what other people think?

Life is short. Far too short to spend it wishing you could do something. If you have always thought to yourself, “I want to be a hacker!” you can start, today! If you have a computer that is fast enough and with enough memory, find a guide and set up your own lab. Download a few vulnerable virtual machine images, segment them off, and start hacking! It really is that easy. If you don’t have a capable machine, you can find walkthroughs that explain how to break the virtual machine images. Start reading walkthroughs for machines labeled easy and read, read, read! Once you get good enough, hack yourself an account on hackthebox.eu. If you are willing to work, you too can be a hacker. Remember that there will always be people who talk shit. If you develop all the skills of a hacker, and your reputation precedes you, the only people crazy enough to talk shit about you will do so behind your back and, like the tree falling in the forest, if you can’t hear it, does their shit talk make a sound?

Dave Collins is an offensive security professional who blogs at whatersauce.com and tweets @ whatever_sauce. The author would like to send love greetz to his wife @punkrawkboss.

---

**Hacker Perspective Submissions Have Closed Again.**

We will be opening them again in the future so write your submission now and have it ready to send!