QnA with TheNotSoCivilEngr

How are you doing in this hard time ? I hope you are doing well!

I am doing well! I have been working hard on my Youtube channel, I just finished working on my 11-part under door tool series which I hope everyone enjoys. I wanted it to be a professional-level 1 hour course that can be taught to almost anyone.

Can you introduce yourself (we all know who you are, but for a sake of a Q n A)?

Hello Everyone! I am TheNotSoCivilEngr (The not so civil engineer) I am a physical security professional and locksport enthusiast. I have been picking locks for about 10 years and got into physical security about two years ago. Since then I have tried to make physical security (with a specific focus on displaying its vulnerabilities) as accessible as possible for as many people as I can.

Can you tell us what is you job exactly (if you can`t at least what it is about).

I cannot say what I do exactly, however I work as a security consultant and red team specialist. I do things on both sides of the spectrum, both working in blue-team risk mitigation as well as red-team risk exploitation. Another thing I do is education. A large part of physical security is in security awareness, and a business is only as good as its people, so I do a lot of security awareness and education for people.

What made you learn and do security?

I first got into security, like many people, by watching Deviant Ollam's talk "I'll Let Myself In: Tactics of Physical Pen Testers" I hadn't ever considered lockpicking to be anything more than a hobby, but after watching that video like many others I was truly enthralled by the idea of doing what he does. From there I began to develop my own skills and produce videos on Youtube of my own security related research and education. Through doing so I crafted a network of people in the industry from the guys at Red Team Alliance (RTA) as well as others within the infosec and locksport communities.

How long did it take you to be where are you now ?

It took me probably two years to get to where I am at now, and I'm really just now getting started in the industry. I was lucky enough to have a location and resources to develop my skills on my own in a hands on fashion (practicing and testing various physical security bypasses). All the while I was listening to audiobooks on social engineering and OSINT to help develop my skills in tandem.

What set of skills does one need for job you have ?

I'd say the most important skill one can have is communication. And I know that sounds like a VERY vague and possibly disappointing answer, but that's the truth. Communication skills are hugely important for several reasons that impact all stages of your career:

1. Communication is important for networking and developing relationships with people in the industry. It's a small industry and the people you know is as important if not more important than the skills you have. Despite the skills in physical security bypassing that I have trained and developed over the last two years, I wouldn't have the job I have now if I didn't make and maintain the relationships that got me the job.
2. Communication is incredibly important for a red team specialist to have because it is directly used in social engineering. This is a little less important than points 1 and 3, but it's a direct use for communication on the job.
3. Being able to effectively communicate the risk and potential loss associated with a security vulnerability or flaw is how change gets made and how you can actually get funding for making things more secure, which is the end goal for both the blue and red teams.

Of course, past this, if you want to get into security it helps to know things from both the blue and red team sides. But be pragmatic about things. I always see people asking questions like "What's the highest security deadbolt I can replace my Kwikset with" when they do not realize that things like lockpicking are not realistic threats. Do some research or take classes to learn things from both sides, just because you want to do only red-team related things does not mean knowledge of how the blue team operates won't help.

What is best way for someone to start learning about security ?

I think this answer has three forms:

a. If you want to go about it without spending any money, subscribe to channels such as my own, Deviant Ollam, BosnianBill and LockPickingLawyer. This will definitely help. These channels will showcase various things related to physical security and can teach you some of the concepts and soft skills related to it. Also follow both r/physec and r/lockpicking on reddit.

b. If you are willing to spend a little bit of money, try getting hands on by purchasing your own bypass tools and hardware (maybe replace the doorknob on your bedroom door with a lever style handle and practice using the under door tool on it).

c. If you have some money to spend, I highly recommend Red Team Alliance (RTA). They are the foremost experts in the field of security and are excellent resources, instructors, and all-around great guys to know. I have attended several of their classes and I know that I will end up taking everything they have to offer. They have extensive libraries of information related to every aspect of red-teaming and physical security and have great hands-on demos in class that allow you to really master the skills.

What set of skills is a must have for a job in Physical security / Alternative: What is something one must now if he wants to learn and do physical security?

Something that one must know if they want to learn and do physical security is that the industry is small, and everyone knows each other. If you want to break into the industry (pun intended) I suggest that you try and start actively engaging in it. Not just by commenting in discussions, but also providing some of your own research or content. I originally started my YouTube channel to showcase my skills and capabilities both in terms of technical skills, but also in terms of communications skills. My YouTube content in combination with the networking I did and relationships I built were what got me to where I am at now.

How can one become physical penetration tester ?

I won't lie, I don't have the answer to this question. Actual physical penetration jobs are very rare. There's a low supply, and a TON of demand. Everyone wants to be paid to break into buildings. Of course they do, that sounds like a ton of fun!

As a security professional you are more likely to be doing security assessments rather than full on red team engagements. The best guidance I can give is to pursue a career in security and as your career develops try and steer it to a path where you can develop the technical and soft skills required to either start your own consulting business, or get hired by a company which has a red team.

What are some books that you recommend for starting in PHS (Physical Security) or security in general?

I am not as well versed in books to recommend, I can however say that one audiobook I am listening to (at the recommendation of one of my subscribers) is "Social Engineering: The Art of Human Hacking" it's a bit antiquated in some of its examples, however it is the gold standard in terms of social engineering.

What is some good tip for doing physical security/ general security, or for people who are interested in it?

Participate in the community. Engage in the discussions, create new solutions, make content for people to consume. Very few people do this in this industry, and those who do (such as myself) quickly get noticed. It's the easiest way to get your foot in the door and set up future opportunities.

One of the users asked this specific question : Can you recommend us some good electronic door lock kit to test on ?

It depends, what specifically are you looking to test? Low frequency / high frequency RFID hacking? Bluetooth or BLE related technologies? I am much more familiar with 125khz and 13.56Mhz RFID hacking (using stuff like ESPKeys and the ProxMark3) You can even build them yourself using Arduino kits for relatively cheap. I think the best way to find electronic hardware for testing purposes is Ebay, just make sure you know what you want and what you are buying.

Can you explain some examples of how USA and European PHS and general security is different on a practical level ?

The United States takes security much less seriously for the most part. Of course we do have high security places such as military bases and the like, but generally security is much less of a concern and is much less developed as compared to European nations. This is because of history, European nations have had hundreds if not thousands of years of war and conflict, as a result security is thoroughly ingrained in their cultures through necessity. The United States is relatively young (Less than 250 years old!) and as a result, we haven't had major wars or conflict on US soil lasting for hundreds of years. This is why you'll find ASSA's and other locks which are incredibly pick resistant on most doors in Europe whereas the United States uses Kwikset and Schlage which are incredibly weak in comparison.

Is there any course/training/certification that you recommend for people who wants to do PHS? (beside SANS)

For physical security I would 100% recommend Red Team Alliance if you have the budget. They also do SANS classes, but you can cut out the middleman and go straight to them for training if you live in the United States. I can't really speak to European countries as I do not have any experience with training companies out there. Certifications and trainings will certainly help you in this industry, but networking and having connections with people in this industry is really the key to getting your start. Make a name for yourself and those opportunities will follow.

Do you look at the security as a science (like law, math, …) or as something practical, and how should people that are starting to learn security look at it (studied like science or to learn it on a practical examples) ?

This is a wonderful question. I have several degrees in engineering, so I tend to look at things from a lens of science. With that said, security is a mix. First and foremost, security should be pragmatic. Security is all about monitoring and mitigating real threats, take for example the lockpicking story from question 6: there's no point in having an ASSA Twin 6000 for your deadbolt if a common criminal will just smash a window to get in.

That being said, when looking at security from a red-team perspective I tend to look at things from a science perspective. For example "How can I physically weaken a locking system?" Is there a way to reverse engineer a lock to determine a potential weakness? Questions like those are much more common when I am attacking things, but they're just as important and the pragmatic ones.

To you, what is more important : having right and many certifications, or knowing right people ? We all now that this world is world where if you don`t have papers for you knowledge it is same as if you don`t have it. But it is also important to know right people at the right time. And to you. Who would you rather hire, person A (who has 4 or 5 certifications but you don`t know how much he likes his work and how much he is passion about it ) or person B ( who you know in person, who doesn`t have any certifications, but you know how much passion he has for that job) ?

I think that question varies industry to industry, however for security I think the answer is readily apparent from my previous ones. I think that its important to have the skills, however since the industry is so small its important to have the connections. Those connections will lead to opportunities which you can then use your skills to secure into jobs.

I would much rather hire someone who has demonstrated the ability to perform the role I am hiring for over a candidate who has several pieces of paper which say they are able to do the job. One candidate actually can do the job, the other has certifications saying they should be able to do the job. That's a huge difference. With that said, certifications are just another thing to help build your resume, I think they are important to show that you have gone through the proper channels, and you even may make connections along the way to getting your certifications which can lead to potential opportunities in the future.

Again, to you, what is more important today, digital or physical security ? We all now both are important but which is more important

I think it depends on what you are trying to protect. In the informational age we are currently living through, securing data is paramount. Companies spend billions of dollars on the most state-of-the-art firewalls, proxies, IDS/IPS, network segmentation, SOCs, etc and they are justified in doing so. You hear about data breaches ALL the time, and truthfully most of these are on the cyber side of things. For as long as you have people involved, phishing will always be an effective digital/social attack. I think that physical security won't get the recognition it deserves until more data leaks which are caused by lapses in physical security occur.

As it currently stands I believe that digital security is more important currently, which is evident from the amount of money spent trying to prevent it as compared to physical security.

Do you think that people are not going for career in security (especially in PHS) because most of population thinks it is easy and it shouldn`t be separate job from other jobs?

I think it's a combination of several factors.

a. I think that when most people think about physical security they think "security guard" and they don't realize how much goes into physical security.
b. There are much fewer jobs in physical security as compared to digital security. Just take a look on any job listing website for digital security and compare the number of results against physical security.
c. Companies do not fully appreciate how important physical security is, as a result its not funded as much as it should be, which means there's less opportunity.

Do you think that is worth it to peruse career in PHS in countries that are not as developed as USA, UK, Germany, or some other big and developed country? For those people it is hard cause countries don`t recognize a need for PHS career cause they are many years behind others.

That's a difficult question to answer because it varies country to country. I think that if you are truly passionate about something you should pursue it regardless of the obstacles. Before I made the transition to security, I was headed toward working a job that I wasn't interested in for the rest of my life. That would have been miserable.

If you live in a country where there are absolutely no opportunities for physical security I would suggest you try and find whatever is the closest alternative and work that. It may not be your first choice but as you work it will allow you to grow your skillset and take the time to develop relationships and opportunities in related (and more interesting) fields.

Is there any interesting story about your lab/office/training space?

I will (hopefully) have a series coming up on stories from the field which will incorporate stories from both myself as well as other industry professionals!

What are you currently working on ?

Well I just finished my massive under door tool series (11 videos, over an hour in total length) I have several collaboration projects in the works, but I also want to get back to my overt entry series as well as my OSINT series. I also have a video focused on social engineering along with some other non series related videos.

What is your biggest success in your career ?

My biggest success in my career was deciding to pursue my passion! It was an incredibly daunting decision because I went from a full time engineering job to zero certainty or guarantee for success in my new endeavor. You spend most of your life working, its paramount that you spend your life working on something you are passionate about.

Where can people find you on internet ?

I'm active on three social media platforms:

a. *Youtube (TheNotSoCivilEngr)*
b. *Twitter (@NotSoCivilEngr)*
c. *Reddit u/TheNotSoCivilEngr*

(also follow and interact with the r/physec subreddit, I've been trying to revive that sub for a while now)

Also thank you NoMan29 for reaching out to me, I appreciate your involvement in the community and the steps you are taking to grow and develop your passions for security.

-TheNotSoCivilEngr