ABSTRACT SECURITY

Date: 11.10.2020.

Interviews with:thesle3p

NoMan29: Welcome everyone! Welcome to tonight`s interview with thesle3p. Hello thesle3p!

thesle3p: hello

N: How are you

t: i am doing well

N: That is nice to hear! Shall we start with the interview?

t:lets

N: Ok, can you introduce yourself?

t: I go by the thesle3p and i work on the red team for a Fortune 50 company and in my spare time i run the New York City Chapter of The Organization Of Lockpickers (TOOOL)

N: Nice! so just to check that is toool.ny?

t: yes

N: Ok then, lets start with some basic ones. How did you get into security, especially Physical Security?

t: when i was in my teens i started hanging out in chat rooms with people who did what we will call `` Network Security Reaserch`` and began to pick up knowladge about that from hanging out there and that led me to me taking up lockipicking as a hobby and when i graduated college my mentor basically told me ``You work for me now `` and i worked as a Penetration tester and then as a red teamer. But the more i went down that path the more i gravitated to the physical security side.

N: Oh that is interesting path. So you had that luck to get in some IRC rooms and learn. Today it is a little bit harded to do that.

t: for sure. That aveneue is much harder now.

N: Yeah, it is hard to find someone who is not trolling you or someone who you can learn from. Now that we are on the topic of your job, tell me did pandemic affected your job in any form or way?

t: my employer has forbid me from going onsite (physical testing) unitl a viable vaccine is available so i am stuck doing network security testing and Research and developmet.

N: Ah yes, well it is good that you are in the digital side too then!

t: that`s something that puts me in a advantegous position. The days of physical sec being siloed from network security are coming to an end. To have a succesful career you really need to be able to do both.

N: Yeah even a little bit. Ok so we tat you love your job (from your talk and from your great tweets), so, do you look at Physical Security more as art or as science?

t: an art for sure, there are aspects of it that requre a scientific approach however. Espeacially on the blue team. But the art of breaking into a building is that...an art.

N: hah interesting! Interesting view! And i agree. SO you said it is more of an art, do you have regime for traning/practice - and, if so, which skills do you priorities on practicing?

t: so physec testing is a interdisciplinary skill meaning you have to understand a wide array of topics ranging from electronic and locksmithing to psychology and graphic arts. Sometimes having the time to maintain and learn new skills is harder than doing the actual work. But at the core of the profession the ability to figure out how things work on your own is the most important thing you can learn. There are a few org that offer traning courses but at the end of the day you have to be able to be your own instructor.

N: Ok so how do you train your understanding of how things work? Do you take one piece of something and try to understand it or ?

t: the best way to learn is by doing. Practice taking apart things and figuring out how they work and then look for new ways to exploit them. One of my favorite ways to do this is purchase a piece of physical security hardware off amazon or ebay etc and take it apart and look for new ways of defeting it. THat way you not only keep your skills sharp you have a shiny new 0day to use if you ever encounter that in the field.

N: hah that is nice way of practicing! I have to remember that one hah Ok now, what does your lab look like? Do you have advice for people looking to set up their own?

t: so right now my lab is a mess because i am in the process of moving home but it`s fairly extensive. I have a bench power supply and vice grip to study electronic access control hardware, badge printers for making pretext props and even some gear for defeating tamper evident seals. It`s constantly growing as the breadth i study grow.

N: wow hah i imagine it is big and detailed table

t: it`s technically two table at this point.

N: haha Now we know that you have many skills, so do you think that it is better to generalize and try and do a bit of everthing, or specialize in one area?

t:i think it is good to specialize in 3 or 4 areas but have basic competency in as many things as you can. I get sd whenever i see people overspecialize themselves into only one area because they end up limiting their potential. Learn as much as you can but find 3 or 4 areas you can be an expert in.

N: Yeah that is a good advice! In your opinion, which is more important: having relevant certs, or knowing right people in right places?

t: nierher, focus on building skills and use those skills to impress the right people in the right places.

N: So do you have any certs? If yes, which ones?

t: i have two certs i got from the CORE group but i didn`t know the courses i took came with certs till after i took the courses. I never put much value in certs to be honest. Skills and interlligence impresses me not certs.

N: but sometimes certs are needed to work in some companies, and honestly that is unfair.

t: it is sad reality. But i would argue that companies that are obsessed with certs are not good placec to work.

N: Ok and what courses would you go if you were starting right now? And which ones would your recommend for starting in PhySec?

t:so because i didn`t go the courses route in the start of my career i don`t think i am the best person to ask which courses are good to start out. That being said the RTA courses are well regarded by many,

N:Would you say that they are good ?

t: sadly i do not.

N: Ok then. Now this questions i found on some post and on some servers so i wanted to ask you, what is RedTeaming to you?

t: red teaming is te art of seeing how well an org`s entire secuirty posture holds up when under attack. The People, the Procedures and the Technology. We let the blue team see what happens when a determined attacker goes after an objective.

N: Ah ok then, and could you explain to us what Purple Teaming is?

t: Purple teaming has become popular lately because it lets blue team look over the shoulder of the red team as we operate so insted of learning how to engagement went afterwards by reading the report the blue team gets to ride along with us and see how we attacked them first hand. I have not dony many purple team engagments but i do see the value.

N: hah.. interesting explenation...

t: in an ideal world the RedTeam helps the blue team make our job harder but the blue team tells us how they caught us if they did so we can make our techniques better.

N: So which skills does someone need to be successful at red teaming?

t:you need to be adaptable as things are changing constantly and you need to be able to think like an attacker at it`s core but you also need to be able to communicate your fidings well. It doesn`t matter what you did or what you found if you report does not give your target enough informations to make things better.

N: true true, so what set of skills would you look for when you want to hire someone?

t: i look for skills that relate to Research as a big part of this work is coming up with new tools and techniques but more importantly i look for skills my team does not already have which is why i think it`s important to pick 3 or 4 ares to specialze in because a good red team birngs in people with a divese set of skills.

N: ok and which resources do you recommend for PhySec and red teaming? And what advice would you give to someone who is just starting?

t: sign uup for as many blue team publications as you can from org like ASIS international or loss prevention magazine even thought they are blue team you can`t do red teaming unless you undrestand how the blue team operates. And i meay be biased but joining a locksport organization such as toools is a good way to meet other people interested in physec which will help you develop new skills.

N: Ok and what is the one thing about your job that makes your heart beat faster?

t: so the only part that really makes me anxious exfilitration. When i am leaving a building i get parinoid ``Did i remeber to do this right? Is a security guard following me? Did i leave something begind or forget to do something?`` - That paranoia only goes away when i wake up the next day.

N: Hah that sounds stressfull. Ok and what is one question that you shish someone would asked you, but never did?

t: i think something i wish i was more aware of strating out was how much drama this community and industry has. THere are a lot of people with big egos making people stressed out just because they can and think it`s counter productive to the growth of the community.

N: Ok and can you tell us if there is any story behind your handle THESLE3P?

t: it comes from two sources. One i have this nasty habit of either sleeping too much or not enough. And also i love the song by NAS ``New York State of mind`` where he says `` i never sleep because Sleep is the cousin of Death``. For the end i just want to say this: The most

important thing to remeber when starting out in this work is never assume things are as hard or compicated as people make it sound. Research it for your self and you will often find it is not as hard as complex as people make it out to be.

END