ABSTRACT SECURITY

Date: 22.09.2020.

Interviews with:Brent White (BITKILL3R)

NoMan29: Welcome everyone! Welcome to another great interview with Brent White! Hi Brent, how are you!

Brent White: I`m well, thanks for asking.

N: I hope you are doing fine during this hard time.

BW:I am. Fortunately, i work from home mostly, so i`ve been good. Have had to make adjustments, as we all have, but doing well over all.

N: That is nice to hear! Shall we start with first question? Can you introduce youself?

BW: Sure. I`m senior Security Consultant ta NTT, Ltd., focusing on physical security, covert entry, and social engineering. I also perform several other engagement types such as network, wireless, and web application penetration assessments.

N: Yeah, i must admit you are on many fronts in Security!

BW: Gotta stay marketable.

N: hah yeah. But i musk ask, how did you get into Security? And especially Physical pen testing ?

BW: When i was in high school, a group of friends were into this thing called ``Phone Phreaking``. I was always interested in electronics, so this really caught my attention. I dove into that, and about that time, the movie ``Hackers`` came out. I tought it was awsome, and it was all over from there. I started teaching myself about *NIX system, digging through the internet to find anything i could, such as the Hacker Quaterly, 2600, Phrack Magazine, online BBS systems, CUlt of the Dead Cow, etc. Because i wasn`t doing things ``ethically``, this led to me getting into a bit of trouble in high school, so i kind of hung it up for a bit. I an avid musician, so i was in several bands in high school, into college. At that point, i thought i was going to be a ``rock star``, and i needed to strat making website for my bands, you know - to get famous. LOL!
Regarding physical security, the company i`m at allows those who are interested in other assessment type to learn them, and jump in to them. I was very interested in physical bypassing, social engineering, etc. and just really dove into in head-first. The rest is history.

N: Ok i must admit that this how you started sounds a little like Kevin Mitnick story haha

BW: Thankfully,not as extreme. No arrests or jail time. Just a healthy heart-to-heart with the principle of the high school that i hacked. HE

asked, i admitted, and we went from there. Needless to say, i washed SEVERAL windows of the high school.

N: Hahaha ok well it paid off!

BW: Indeed.

N: How has pandemic affected your work.

BW: Well, it is very difficult to break into a building while you`re still at home.

N: hah well yeah.

BW: I haven`t quite mastered the power of being Omnipresent yet. Until then, or until this quarantine subsides, i have been focusing on remote network peneteration assessments. I enjoy those, so its been nice to sharpen my skill set with that. It has also been very nice to have a long break from traveling, after doing it so much for several years.

N: Yeah this time is good to practice those skills. Do you look at PhySec more as art or science?

BW: Great question! I see it as both. WHen you are dealing with the physical bypass and electronics side of things, there is a science to it. Those are mechanical devices or computers that function in specific way. However, there is a bit of art that goes into the creative side of vreating bypass tools to overcome those devices. You need to be able to creative and think in an untraditional manner.

N: hah i agree. it is little of both. And in your opinion, which is more important: having relevant certifications, or knowing right people?

BW: Ah this is one of those ``stir the pot`` questions, because so many people have had so many different experiences. So, i just want to clear that this is only my opinion, and it`s based off of my own personal experience. It will not apply to everyone. WHen i started this career, i did not have certificaitons. When i was brought onboard at NTT, which was SOlutionary at the time, it was because of my long-time friend, Tim Roberts. He and i learned about phone phreaking, hacking, etc. together as kids, and have stayed in touch throughout the years. He got me the initial interview when there was an opening. So, knowing him helped me to get my foot into the door of the company.
From there, beacuse i am passionate about sharing what i have learned about physical security, web hacking,etc... I was able to start meeting and ``knowing the right people``, which lead to more opprotunities such as being on the DEFCON Groups board, being a trusted advisor for the TN Dept. of Safety and Homeland Security, and much more.
Networking has been a HUGE part of my career, and it is certainly an area that should not be overlooked.

N: Yeah i understand. Everyone is different. And what courses would you taking if you started now? If you could do it all over again.

BW: I would focus on being able to pass the OSCP cert from Offensive Security. There are several online resources to help you get your skill level up to this, such as HackTheBox. THis is if you`re wnating to becoming a security consultant, or security researcher. It`s a well-respected hands-on cert. For physical security, this is a bit of a tough one. You`ll need to make sure that whenever you work provides you the opprotunity to perform these assessment types. Get your feet wet. If you like it, dive in. THere are also other paths for physec-related careers such as military, government, and law enforcemnet.

N: Yeah many people don`t know how to get started or what courses to take. Do you think it is improtant to go only on courses that give you certs? Or do you think that others that don`t give you cert are good or better yet worth it.

BW: I don`t think that you should limit yourself to only things that provide certs. I would just make sure that whatever you`re taking is relevant and strengthiening your skills in a way that is fun for you.

N: Which skills does someone need to be successful at physical pen testing? - i know that this question you get a lot but can you tell us what skills, to you, one must have if he wants job of PhyPenTester.

BW: Assuming phy pen testing also involves social engineering and human interaction, the most imporatnt skill is the ability to deal with people. What i mean is that if you are tasked with a covert entery assignment and your goal is to gain access to an area of a facillity, how are going to perfomr when you are engaging in conversation. Are you going to keep your cool ? Are you able to respond to a question or challenge in a manner that is belivable, or will they see that you are nervous and fumbling over your words? Can you improvise easily? The technical skills to bypass security access control can be learned mych more easily that trying to teach someone how to act around people when this just might not be a part of their personality.

N: Yes, i agree. As FC said to be confident but not dickhead confident.

BW: Exactly.

N: Ok and what skill set are you look for when hiring someone ?

BW: Thier drive and honesty. If they clearly don`t know the answer to a questino and are just trying to make something up i nhopes of saying the right thing, this is a red flag. I like people who are okay with saying that they do not know, but they are willing to learn. It`s also extremely important to have good ``soft skills``, such as the ability to interact well with clients. You can be an absolutely brillian hacker, but if you are not good at communication and show taht you hate dealing with people, it`s going to be a very hard sale. At least in the consulting world.

N: yeah, well anywhere if you don`t know to deal to people you will not get job.

BW: Haha, true!

N: What is more important today, digital or physical secuirty?

BW: I think this depends on the situation. If you`re talking about Fort Knox, then the answer would be physical secuirty. If you`re talking about an online retailer, then digital. However, they go hand-in-hand. If one is severely lacking, then the other will suffer. FOr eample, if the online retailer has a hadened externally-facing network, but allows people to just walk in off of the streeet and plug into thier network, or steal a laptop, that`s a whole different set of issues.

N:Yeah i like that. They go hand i hand. So if someone is watching/reading this, and wants to get his/her feet wet in PhySec or InfoSec world, which resources do you recommend?

BW: If i can be selfish and biased for a minute, then i`d recommend www.wehackpeople.com, which is a collection of my research, blog post, and conferences presentations from Tim and I.
In addition, Red Team Alliance provides great traning for several areas of phy sec. Deviant Ollam is also a well known online resource with his presentations. Anything that`s lock-picking related is also helpful. I know that ther eare several more, but i`m blanking at the moment.

N: yeah it is a great web site ! But i have one off topic question. WHy sheep ? I mean logo for for wehackpeople has logo of black sheep if i am not mistaking.

BW: That is correct. There is few different meanings behind it. One, in social engineering, you will hear people refer to others as sheep, meaning those who just follow the masses and don`t think for themselves. The other meaning is that it is a black sheep, meaning that it doesn`t fit in with all of the other white sheeps. It is unique.

N: hah yeah, awsome, nicely done! Now while i was researching for this interview,i have stumble upon your large collection of covert entery tools and covert entery closet (but not the serial killer one). Can you explain what it is for the people who don`t know what i am talking about.

BW: LOL!! My covert entery closet is just a very well-organized culmination of tools that i use for covert entery. It contains several bypass tools, even custom build, as well as items such as keyloggers, network implants, badge cloners, research, and more. My friend Blake with Low Voltage Nation did an on-site interview with me where i went through some of the items in there and what they are used for. The ``serial killer`` part is the unfortunate nickname that my wife gave it. I used to ave a few camping tools such as my hatchet and some knives. And then of course ther are other wires from the under-the-door tool, and other bypass tools. So,she said it looked like something a serial killer would have. And for the record i am NOT a serial killer. LOL!

N: haha it is very impresive.

BW: I`ve updated it quite a bit since that interivew. I need to post some pictures to show the changes. Perhaps i can get to that this week.

N: And to someone who is maybe not in PhySec it really looks like something from horror movie haha But what would you say is your favorite tool from your big selection?

BW: Hands down, the plastic shim. I`ve gotten into more ares with this simple attack than anything else. Other things would have worked as well, but this is so fast so easy to carry, that i often don`t have to try other things on the doors where this is successful.

N: hah ok simple item but it works. You are on every front of PhySec: SE, lockpicking, covert entery,... what is your favorite section of PhySec?

BW: Oh taht is an easy one, covert entry.

N: Yeah haha that is what i tought haha. Now you have shared your EDC with us, i wanted to ask you what EDC set do you recommend for beginners?

BW: if this is for beginners in covert entery, then i wolud recommend someting similar to my wallet. The multi tool takes a little getting used to as fas as holding the lock picks a little different. If you are not performing covert entery, then the multi tool is overkill. The wallet would suffice as it contains basic lock picks, the door shim, sparrows hall pass, and couple shims. I`d also recommend the knife that i posted about. I don`t go anywhere without it.

N: Ok. We can see that you like your job. But can you tell us of many things you do, which one makes your heart beat fastest?

BW: Covert Entery. The initial moment before i deciede to attemt entery into a building for the first time. Did i prepare enough? is my guis convincing ? I am composed? But i enjoy it. I enjoy the preparation for it, and the actual entery. I also theaching and traning others for it as well. My least favorite is the report writing.

N: hah okay, and what is the easiest assessment you ever done ?

BW: After-hours entery into a company`s suite in a shared building. The keypad code was guessed on the 13th attempt, sensitive data was lying around. The locks on the shredder bins were crap. THe secuirty guard was supposed to be remotely monitor the cameras, but clearly was not. We were in there for a couple of hours, basiclly just waiting for someone to come. After a wile, i started doing jumping jacks in fron of the security camera at the front door and really acting stupid, but that still didn`t work.

N: hahaha ok that is really funny.

BW: They were not happy. Theye were very convinced that the security company was on-point.

N: Can you tell us what is the story behind the name BITTKILL3R?

BW: Originally cowerkers were calling me B33f, because i enjoy weight lifting. But as we know there`s already a popular framework out there with this name. So, BITTKILL3R just kind of came about as spin off of jokes about my being ``Lenny`` from ``Of Mice and Man``. You know, ``i wanna pet the rabbit`s, George.``, and accidentally killing the rabbit from squeezing too hard. I try to muscle everything, i guess? The ``Bit`` part was relative to hacking.

N: hah interesting. And what is the one question that you wished someone has asked you, but never did?

BW: When i was in high school, i wish someone would have asked me, where do you see yourself in five years? in ten years? I didn`t really have a plan, and because of that, i feel like i missed out on some good opportunities. Thankfully, my awsome wife really helped me to get on a good path presonally and professionally.

N: that is nice to hear. And in some way we have to thank your wife cause if there wasn`t her maybe we wouldn`t have here ! and last question is where can people find you?

BW: I`m on twitter at @brentwdesign, as meniton earlier, i also have website www.wehackpeople.com. We also have a facebook page, which is liked from our website. I have also recently spun up the sub-reddit of r/CovertEntery.

END