ABSTRACT SECURITY

Date: 17.10.2020.

Interviews with:autom8on

NoMan29: Welcome everyone!Welcome to the interview with autom8on

autom8on: ~waves~

N:Hi, how are you? are you doing fine?

a:Yeah, I`ve had a nice lazy day.Done a bit of cooking, done a bit of tidying, played a little PS4, and now here for this. I`ve had worse days.

N:Hah, i am glad, i see you are doing fine! Those days are favorite of mine hah

a: I make the most of my weekends - trying to relax before work starts again tomorrow.

N: Now, can you introduce yourself cause maybe someone doesn`t know who are you are what do you do. Which is hard to find but non the less.

a: Yeah, sure. So, my name is Steve- but i`ve gona by the handle autom8on for years. By day, i work on the offensive security team at large telco. Outside of work, i`m the CEO of Moon on a Stick Lock Picking and Cold Brew Coffee Emporium, i help run DC Gloucester, help run SnoopCon, and generally mess around with locks.

N: Hah you are all around the place!

a: Oh, and i`m an assessor for the TigerScheme qualifications.

N: Wow nice, can you tell us what is TigerScheme qualification?

a: Yeah - so, in the UK there is qualification know as CHECK, which is run by the government to make sure people are appropriately qualified to test governments systems. There are now 3 equivalent qualifications that can get you CHECK status - CREST. CyberScheme and TigerScheme... It`s basiclly pen test exams.

N: Oh wow, it is nice to hear that there is something like that hah

a: But there`s quite a big ongoing effort to rewrite the exames and get them online, due Covid.

N: yeah yeah i understand

a: SIncce they always used to be assessed in person.

N: And is there a practical part?

a: Yeah - so there are junior and senior exames. But both have multiple choice questions, essay queastions, and a practical assault course you have to hack.

N: oh wow nice

a: Junior exame is a day. Senior is 2 days.

N: I am impressed.

a: It`s been around (CHECK)for a long time, so it is well established over here. Started in the late 90`s. The MoD were well ahead of the curve with pen testing.

N: I mean i belive that therer is similar things all around the world, but i have neve heard about them.

a: Yeah, CREST are certainly doing things on global scale now.

N: oh ok i have to look it up. I have never heard about it.

a: Yeah, i don`t think CHECK really is known outside of UK testing circle.

N: Yeah. Ok so you said that TS is affected by Covid, is your work affected too?

a: Yeah, it hasn`t been a good year. My on-site work has basically been cancelled or postponed. So instead i`ve been working on some more cybery stuff. We still have travel restricitons in place now. SO aren`t expecting much to happen this side of Xmas.

N: Yeah that is sad...But hey it works out that you know cyber stuff

a:As weel as getting involeved in the RT breaking in type work, i also get involved in less offensive physical audits - and they`ve stopped too. Oh, yeah, i`ve got 20+ years to of hacking skills to fall back on.

N:Hah wow and that is wow haha

a: Doing a lot of OSINT discovery and large scale VA work in the meantime. Not nearly as good fun physical work- but it pays the bills!

N: Nice, so if you have that much IT background, why PhySec (Physical Security)?

a: Oh, i also do a lot of mentoring and teaching - that is quite busy too.

N: i like that!

a: Well- it started out just as a hobby, years and years ago when i was working for the MoD. Someone taught me how to pick locks- so i became

that guy who could open your filing cabinet in the office when you forgot your keys. Then i started buying more and more, as you do.

N: Haha, and you fell in the rabbit hole.

a: Then i started doing little talks and workshops at conferences, and it just grew from there. But also, my role has changed. As we`ve moved from pentesting more into more red team work - we`ve had to develop the physical side of our skills too. So i`m lucky that work has funded quite a bit of traning..We have a small, but well trained team.

N: Nice!

a: I am just the one who is utterly obsessed with locks. Fortunately, my employer takes secuirty seriously.

N: Ok and do you have any regime on how do you practice it? And side question, do you still practice Cyber Sec?

a: It`s tough. I`m really bad in terms of spending time studying the theory, but dodging the pracitce. I should practice more than i do. I need to draw up a proper timetable and stick to it. I`m supposed to be setting some practie/traning stuff up at work, but that`s been postponed along with all our onsite work.
Yeah - i spend a lot of time still practice the cyber sec side of things. We use Immersive Labs a lot at work as traning platform - but I also play around on Hack The Box, and others.

N: Oh wow ok, as i said you are really all over the place haha

a: Although the physical side of the job is in increasing as time goes on - we still do a lot more cyber stuff then purely physical.

N: Hah, nice. And do you have lab where you pracitce PhySec or?

a: So i have a bunch of stuf at home. I`m currently in the procces of re-arranging my workshop again. For work - i`m supposed to be setting up a physical location for practice. I moved in a couple of days before lockdown started - so, again, that`s on hold for now. But we`re looking to create an inhouse facility where we can practice all the relevant skills for the job.

N: hah nice to hear that.

a: To make sure we don`t have skill fade in between training sessions,

N: And can you tell us, what is something that is essential for you training, it can be a thing, a ritual of some sorts, habit,...

a: So i guess it`s the drilling of practical skills in realistic scenarios. It`s one thing to learn how to open a lock in classroom setting - it`s a completely different doing it outside in the middle of the night when it is raining. I`m keen tot do as much practice as possible before you need to do something for real. ONce you`ve planned a

job - you practice and practice and run little drills. To make sure it`s second nature when you come to actually do it.

N: Huh nice, that is actually very nice!

a: It`s natural to make mistakes during traning. It`s important to learn from them. So, better to make those mistakes on a practice run than the rael job.

N: Yeah, make mistakes during the traning not during the real thing.

a: the old ``traing hard, fight easy`` thing.

N: Yeah. Now i know that you are biased but that me what is your opinion about certs?

a: lol . I guess they are a necessary evil sometimes. Like over here - there is work you can only do if you have a valid CHECK cert. But some are better than others. I`m big fan of stuff like OSCP - due to the practical nature of it. Less so stuff like CISSP or CEH. I`m more interested in people with practical skills than theory.

N:ok so certs or right people ?

a: Same with studying. I have a degree, but i don`t use most of the stuff i was taught. I know some amazing people who don`t have academic qualifications. Also know some idiots who do!

N: haha ok i understand.

a: But the job market is becoming so busy - somtimes you need a qualification or a cert just to get your foot in the door.

N: yeah ok understandable.

a: So, i`m torn. I see both sides.

N: Now, as a red teamer, what would you say someone (who is starting) needs to learn? what skill? what skills does one need for red teaming?

a: Well, that depends on what definiton of ``red teaming`` you are using. From my perspective - it`s bleded electronic/physical attack - so you have options on whether you want to focus on the physical side or the electronic. This also leads onto the whole ``specialist or generalist`` questions. I started out on the cyber side, and am now moving to more physical stuff - so it`s natural for me to suggest that people might find it easier following a similar path - worry about the IT stuff first, and the physical later.

N: huh interesting.

a: But then, if it`s SE you`ve interested in, that`s probably bad advice.

N: Hah well there is SE in Cyber Sec too.

a: There is such a wide variety of sklls.

N: Yeah you have to choose to see what is your interest and to follow it.

a: I think finding real people who are working in the field, and getting to know what stuff they are up to (that they can tell you) is a wise move. Hence why i`m happy to sit on this server and chat to people.

N: Hah yeah i agree with you! that is one of the best ways to learn something. Honestly that is why i made this server, so i agree with you.

a: But, ultimately, be prepared to do whatever needs doing. If you are coming in as a junior - expect to get all the works that nobody else wants to do.

N: but i must ask you - which one do you support, knowing everything in general or specializing at one thing ?

a: So my view has changed massively over time. When i started, there was just less to know. It was easier to be a generalist. Now there is just so much potential specialisation - that i prefer to focus on what interests me, and leave the rest to other people. It`s one of the great things about working on a good team - you can rely on other people to do thier bits well and i just focus on doing mine. Buti think that i`m lucky to be working where i am. I know that my view of the world is quite different to some people. My employer is supportive of what i want to do. It`s taken me more than 20 years to get here, however.

N: Yeah but it would be very boring if we all tought the same and talk the sameme too right?

a: Very true! I think you have to draw a line somewhere. There is too much technology emerging every day to be an expert in everything.

N: Ok now, which resources would you recommend to some who is just starting? where to look at, what to do,...

a: So i spend an inordinate amount of time around various Discord Servers, slack channels and signal groups - as well as lost of time randomly disapperaing down rabbit holes thanks to twitter and youtube... Also reading a lot of books when i can. There is so much informations available today, compared with when i started. Oh podcasts too.

N: Basically just hang around the people who do the job and wnat to and talk to them and read and listen about it.

a: if you can find them. But yeah - study as much as it is possible. Go to conferences. Also get involved in community stuff, with like minded individuals. I`m far more impressed by someone who has actually contributed to open source projects, than just got good academic qualifications.

N: Ok and now a little bit of personal questions. What is your favorite part in your work? And what is your least favorite?

a: Spending someone else`s money is always nice. Work finacecs tranings and tools taht i`d never be able to afford myself. I also get to see some interesting things. That is worth more to me that money any day.
In terms of worst - the bureacracy.
Working for a massive organistaion means things can sometimes be difficult to get done. Red tape, paperwork, ...

N: ah ok i understand. And what is one thing about your job that makes your hearth beat faster?

a: It`s impossible to describe the nerves you have when you`re trying to conduct a large scale physical incursion... and how amazingly good it fels when everything finally clicks into place and the plan works.

N: HAh yeah when you plan it well! Ok and what is one question that you wish someone would asked you, but never did? (related to Physical Security)

a: ``Who are you, and what are you doing here ?`` lol

N: Ahahahaha ok that is such a good question haha

a: The really scary thing - when we started doing physical testing - was the fact taht nobody ever asks you who are you, or why you are here? Like we`ve been intreruppted by security guards before - who`ve just said hello, then left us alone - whilst we were in the middle of wiring a drop box under a raised floor.

N: Hah yeah i understand. Such a easy question but nobody every asks it.

a: Most people don`t cary about security. It`s not their job. They just want to do thier job 9-5 then go home.

N: yeah.

a: They assume if you have badge on you must be legite.

N:Again, we`ve had arguments with security guards who refues to belive that the passes we`d made ouselves weren`t genuine. They aren`t trained to spot forgeries.

N: yeah... now can you tell us if ther is story behind your handle AUTOM8ON?

a: Yeah, there is. It goes back to when i was working for the MoD - and i used to read a lot of hacking newgroups, specifically alt.ph.uk. There was a guy on there who notice i kep going and looking at his webserver every time he posted anything to the group. He was spotting our proxy in his log. He tought he was being targetted by an automated scanner, but he wasn't, it was me. So, i became known in our office as the automated scanner - which got shortened to autom8on for our office quake server.

N: hah interesting!

a: I am autom8on on twitter by the way- but i don`t tend to look at that account, and insted use @a8n_pub for public stuff. I also go by ``Security Nihilist`` - after something that Haroon Meer said about me in a 44con keynote once.

N: haha ok, now let`s see if anyone has any questions for you!......What is your favorite lockpicks brand and style?

a: So, currently, for pin tumbler type locks - i`m currently favouring a Law Lock Increment Pro set, as i llike the over sized handles - www.lawlocktools.co.uk//The-Increment-Pro-Lock-Picking-Set
In terms of dimple picks- i am currently testing our just about every set i can get my hands on. Current favorite for balance on price/quality is probably the Huk set - though, like with any tools, i expect to have to do a bit of work to make them more usable. I guess - i should stress the point - you don`t need expensive tools to develop skills, i waste lots of money on tools. Cause i like shiny things!

END